IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES
(Attorney Docket № 14222US02)

In the Application of:

Martin Lund

Serial № 10/647,963

Filed: August 26, 2003

For: SYSTEM AND METHOD FOR INTEGRATING MULTISERVER PLATFORMS

Examiner: BARQADLE, YASIN M

Group Art Unit: 2153

Confirmation № 5243

Electronically filed on 16-JUNE-2008

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from an Office Action dated December 14, 2007 ("Final Office Action"), in which claims 1-15 were finally rejected. The Applicant respectfully requests that the Board of Patent Appeals and Interferences ("Board") reverses the final rejection of claims 1-15 of the present application. The Applicant notes that this Appeal Brief is timely filed within the two-month period for reply that ends on **June 16, 2008** (the Office date of receipt of the Notice of Appeal being April 16, 2008).

REAL PARTY IN INTEREST
(37 C.F.R. § 41.37(c)(1)(i))

Broadcom Corporation, a corporation organized under the laws of the state of California, and having a place of business at 5300 California Avenue, Irvine, California 92617, has acquired the entire right, title and interest in and to the invention, the application, and any and all patents to be obtained therefor, as set forth in the Assignment recorded at Reel 014447, Frame 0015 in the PTO Assignment Search room.

RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

The Appellant is unaware of any related appeals or interferences.

STATUS OF THE CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

Claims 1-15 were finally rejected. Pending claims 1-15 are the subject of this appeal.

The present application includes claims 1-15, which are pending in the present application. Claims 1-15 stand rejected under 35 U.S.C. § 102(b) as being anticipated by CISCO Systems, Virtual LAN Communications, http:/./web.archive.org/web/19990209172148/cio.cisco.com/warp/public/614/13.html, July 14, 1995 (hereinafter, CISCO). *See* Final Office Action at pages 4-11.

The Applicant identifies claims 1-15 as the claims that are being appealed. The text of the pending claims is provided in the Claims Appendix.

STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

The Applicant has not amended any claims subsequent to the final rejection of claims 1-15 mailed on December 14, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))

The invention of claim 1 is illustratively described in the Specification of the present application in, for example, "Brief Summary of the Invention" section in page 4 as amended on page 2 of the Applicant's Response to Office Action filed September 26, 2007. Certain embodiments of the invention provide a method and system for communicating information in a server platform. *See* the present application at page 4, lines 2-3. Aspects of the method for communicating information in a server platform may include receiving at least one packet from at least one of a first switch blade associated with a first multiserver platform. *See id.* at page 4, lines 3-6. The method may also include determining a [ ] server blade associated with a second multiserver platform that may receive at least a portion of the received packet. *See id.* at page 4, lines 6-8. In this regard, at least a portion of the received packet may be routed to the [server blade]. *See id.* at page 4, lines 8-9.

Claims 2-4 are dependent upon claim 1.

The invention of claim 5 is illustratively described in the Specification of the present application in, for example, "Brief Summary of the Invention" section in page 4 as amended on page 2 of the Applicant's Response to Office Action filed September 26, 2007. Another embodiment of the invention may provide a machine-readable storage, having stored thereon, a computer program having at least one code section for communicating information in a server platform. *See id.* at page 4, lines 15-17. The at least one code section may be executable by a machine, thereby causing the machine to perform the steps as described above for communicating information in a server platform. *See id.* at page 4, lines 17-19. Aspects of the method for communicating information in a server platform may include receiving at least one packet from at least one of a first switch blade associated with a first multiserver platform. *See id.* at page 4, lines 3-6. The method may also include determining a [ ] server blade associated with a second multiserver platform that may receive at least a portion of the received packet. *See id.* at page 4, lines 6-8. In this regard, at least a portion of the received packet may be routed to the [server blade]. *See id.* at page 4, lines 8-9.

Claims 6-8 are dependent upon claim 5.

The invention of claim 9 is illustratively described in the Specification of the present application in, for example, "Brief Summary of the Invention" section in page 4. Aspects of the system for processing information in a multiserver platform may include a first multiserver platform having a network interface and/or a first switch blade. *See id.*

at page 4, lines 20-21. At least a second multiserver platform comprising a second switch blade may be coupled to the first switch blade of the first multiserver platform. *See id.* at page 4, lines 22-23.

Claims 10-15 are dependent upon claim 9.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Claims 1-15 stand rejected under 35 U.S.C. § 102(b) as being anticipated by CISCO Systems, Virtual LAN Communications, http:/./web.archive.org/web/ 19990209172148/cio.cisco.com/warp/public/614/13.html, July 14, 1995 (hereinafter, CISCO).

ARGUMENT
(37 C.F.R. § 41.37(c)(1)(vii))

In the Final Office Action, claims 1-15 stand rejected under 35 U.S.C. § 102(b) as being anticipated by CISCO.

I. Claims 1-15 Are Not Anticipated by CISCO

Claims 1-15 stand rejected under 35 U.S.C. § 102(b) as being anticipated by CISCO.

A. Rejection of Independent Claims 1 and 5

The Applicant turns to the rejection of claims 1 and 5 under 35 U.S.C. § 102(b) as being anticipated by CISCO. The Applicant submits that CISCO does not disclose or suggest at least the limitations of "receiving at least one packet from at least one of **a first switch blade** associated with **a first multiserver platform**; determining at least **a server blade** associated with **a second multiserver platform** for receiving at least a portion of said received at least one packet; and routing said at least a portion of said at least one received packet to at least **said server blade**," as recited by the Applicant in the independent claim 1 (emphasis added).

With regard to "receiving at least one packet from at least one of a first switch blade associated with a first multiserver platform," the Final Office Action states "see Page 9, Figure 9, left hand side bottom switch is first blade switch and multiserver platform is one under label VLAN1; it is inherent with network interface that any packet

originated by the multiserver will be received by the first blade switch." *See* Final Office Action, Page 4, Lines 12-16. **However, CISCO fails to disclose a first switch blade or a first multiserver platform. Rather, the CISCO publication discloses using the Catalyst 5000, Catalyst 1200 and ProStack switches, which are not switch blades. *See* Evidence Exhibits 2, 3 and 4 for Catalyst 5000, Catalyst 1200 and ProStack product information and other related documentation. <u>By explicitly teaching to use non-blade switches, CISCO clearly teaches away from using "a first switch blade" as set forth in Applicant's independent claims 1 and 5.</u>**

Additionally, the Applicant notes that claims 1 and 5 recite "receiving at least one packet **<u>from at least one of a first switch blade</u>** associated with a first multiserver platform." Thus, the Examiner's assertion that "it is inherent with network interface that any packet originated by the multiserver will be received **<u>by the first blade switch</u>**" is irrelevant. The Final Office Action fails to show where CISCO discloses "receiving at least one packet **<u>from at least one of a first switch blade</u>** associated with a first multiserver platform," as set forth in Applicant's independent claims 1 and 5.

The Applicant further notes that the only servers disclosed in CISCO's Fig. 9 are in the bottom right hand corner. The computer icon is used in the CISCO publication to show "end stations" and the file cabinet is used to show a "server." *See e.g.*, Figs. 2, 5, 7 and 9. The Examiner acknowledged the difference between workstations (i.e., the computer icon) and servers (i.e., the file cabinet icon) in the Response to Arguments section of the Final Office Action where the Examiner stated that "VLANs as in fig. 2 show a multiple VLAN groups of an enterprise network that include Engineering VLAN,

Marketing VLAN and accounting VLAN **each with its own workstations, servers connected via switch devices**." *See* Final Office Action, Page 3, Lines 10-13 (emphasis added). Clearly, at least Fig. 9 of the CISCO publication differentiates between "end stations" and "servers." Thus, the computer icon under VLAN1 in the bottom left hand corner of Fig. 9 cannot be a multiserver platform as alleged by the Examiner. Further, nothing in CISCO indicates that the VLAN1, VLAN2, or VLAN3 servers in the bottom right hand corner of CISCO's Fig. 9 are multiserver platforms or part of a multiserver platform. A multiserver platform is described in Applicant's specification in, for example, at least Figure 1 and accompanying text in paragraphs 22-28.

With regard to "determining at least a server blade associated with a second multiserver platform for receiving at least a portion of said received at least one packet," the Final Office Action states the following:

> [S]ee Page 9, Figure 9, The **second blade switch is left top switch** and multiserver platform is the one under VLAN1; when a packet is received from first multiserver platform is received by the switch, the switch will determine (determination is made by rules set by administrator) if the packet is to be sent to second multiserver platform, "Both of these techniques examine the packet when it is either received or forwarded by the switch. Based on set of rules defined by the administrator...", Page 3, third Para, lines 4-6).

See Final Office Action, Page 4, Line 19 – Page 5, Line 6. However, nowhere in CISCO is there any disclosure regarding a server blade and the Final Office Action fails to mention a server blade. It appears that the Final Office Action confuses a "server

blade" with a "second blade switch." A server blade is different than a switch blade. (See e.g., Applicant's Figure 1 Blade Server 120 compared to Switch Blade 140 and accompanying text in paragraphs 25-27). Further, as discussed above, nowhere in CISCO is there any disclosure regarding a switch blade or a multiserver platform.

With regard to "routing at least a portion of said at least one received packet to at least said server blade," the Office Action states the following:

> **Once the determination is made by the first blade switch, that packet belongs to multiserver platform connected to second switch blade, it will be sent (routed to second blade that is associated with second multiserver platform**, "Based on the set of ruled defined by the administrator, these techniques determine where the packet is to be sent, filtered, and/or broadcast.", Page 3, third Para, Lines 5-7. See also page 9, first paragraph for end-user VLAN information and identification carried between switches, routers, and directly attached servers.

See Final Office Action, Page 5, Lines 8-17 (emphasis added). The Examiner asserts that the packet is routed from a first blade switch to a second switch blade associated with a second multiserver platform. However, as mentioned above, it appears that the Final Office Action confuses a "server blade" with a "second switch blade." A server blade is different than a switch blade. *See e.g.*, Figure 1 Blade Server 120 compared to Switch Blade 140 and accompanying text in paragraphs 25-27. Nowhere in CISCO is there any mention of a server blade, let alone "routing said at least a portion of said at least one received packet to at least said **server blade**," as set forth in Applicant's independent claims 1 and 5.

Accordingly, independent claims 1 and 5 are not anticipated by CISCO and are allowable. Furthermore, the Applicant reserves the right to argue additional reasons beyond those set forth herein to support the allowability of claims 1 and 5.

B. Examiner's Response to Arguments

The Examiner states the following in the Final Office Action:

> Examiner notes that switch blade is a device that performs switching functions (normally at layer 2 of the OSI model). ... As such the switches in Cisco document meet the functions performed by the Applicant's claimed switch blades.

See Final Office Action, Page 2, Lines 10-11 and 13-15. The Applicant points out that with regard to the anticipation rejections, MPEP 2131 states, "[a] claim is anticipated only if **each and every element as set forth in the claim is found**, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 2 USPQ2d 1051, 1053 (Fed.Cir. 1987) (emphasis added). MPEP 2131 also states, **"[t]he identical invention must be shown in as complete detail as is contained in the ... claim**." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

The Examiner does not contest that CISCO is silent as to a switch blade. Rather, the Examiner asserts that "the switches in Cisco document meet the functions performed by the Applicant's claimed switch blades." Thus, using the Examiner's

reasoning with regard to, for example, "receiving at least one packet from at least one of a first switch blade associated with a first multiserver platform," any device that sends at least one packet could be considered "a first switch blade" because that device would allegedly "meet the functions performed by the Applicant's claimed switch blades." Clearly, CISCO fails to disclose each and every element as set forth in Applicant's independent claims 1 and 5, as required by MPEP 2131 because CISCO at least fails to disclose "a first switch blade." Further, CISCO fails to teach the identical invention in as complete detail as is contained in independent claims 1 and 5, as required by MPEP 2131 because CISCO at least fails to disclose "a first switch blade."

Further, the Applicant notes that "switch blade" is a known term in the art. As already stated above, CISCO does not disclose the use of a "switch blade." Even a broad interpretation of CISCO cannot overcome at least this deficiency.

The Examiner further states the following in the Final Office Action:

> As to the issue of server blades and the multiserver platform, the Cisco reference teaches "The backbone commonly acts as the aggregation point for large volumes of traffic. It also carries end-user VLAN information and identification between <u>switches</u>, routers, and directly <u>attached servers</u>." (Page 9, first paragraph. See also *Figure 7: Servers as Part of* Multiple VLANs). It is also noted that VLANs as in fig. 2 show a multiple VLAN groups of an enterprise network that include Engineering VLAN, Marketing VLAN and accounting VLAN each with its own workstations, servers connected via switch devices.

See Final Office Action, Page 3, Lines 4-13 (emphasis in original). With regard to "a server blade," the Applicant notes that nowhere in the Examiner's Response to Arguments section of the Final Office Action is there any identification of "a server

blade" in CISCO. Rather, the Response to Arguments section of the Final Office Action merely points out that CISCO discloses servers. Nowhere in CISCO is there any mention of "a server blade." Thus, CISCO clearly fails to disclose each and every element as set forth in Applicant's independent claims 1 and 5, as required by MPEP 2131 because CISCO at least fails to disclose "a server blade." Further, CISCO fails to teach the identical invention in as complete detail as is contained in independent claims 1 and 5, as required by MPEP 2131 because CISCO at least fails to disclose "a server blade."

Further, the Applicant notes that "server blade" is a known term in the art. As already stated above, CISCO does not disclose the use of a "server blade." Even a broad interpretation of CISCO cannot overcome at least this deficiency.

With regard to "a multiserver platform," the Applicant notes that the Examiner's Response to Arguments section of the Final Office Action merely discusses CISCO's disclosure of using more than one server. However, the use of more than one server does not necessarily mean using a multiserver platform. For example, the Applicant's specification discusses the disadvantages of using multiple single servers in at least paragraphs [06] and [07]. Nowhere in CISCO is there any mention of using multiserver platforms. Thus, CISCO clearly fails to disclose each and every element as set forth in Applicant's independent claims 1 and 5, as required by MPEP 2131 because CISCO at least fails to disclose "a multiserver platform." Further, CISCO fails to teach the identical invention in as complete detail as is contained in independent claims 1 and 5,

as required by MPEP 2131 because CISCO at least fails to disclose "a multiserver platform."

Further, the Applicant notes that "multiserver platform" is a known term in the art. As already stated above, CISCO does not disclose the use of a "multiserver platform." Even a broad interpretation of CISCO cannot overcome at least this deficiency.

C. Rejection of Dependent Claims 2 and 6

Claims 2 and 6 depend on independent claims 1 and 5, respectively. Therefore, the Applicant submits that claims 2 and 6 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claims 1 and 5. The Applicant also submits that CISCO does not disclose or suggest at least the limitation of "wherein said receiving further comprises receiving said at least one packet by at least one of a second switch blade associated with a third multiserver platform and a central switch," as recited by the Applicant in claims 2 and 6.

With regard to claims 2 and 6, the Final Office Action states the following at page 3:

> The method and computer according to claim 1 and 5 (see supra for discussion of claims 1 and 5), wherein said receiving further comprises receiving said at least one packet by at least one of a second switch blade and central switch (see figs 3; 5 and Figure 9) it is inherent in the FDDI a packet on the ring will be received by all members of the ring.

See Final Office Action, Page 5, Line 19 – Page 6, Line 2. For reasons similar to those discussed above with regard to claims 1 and 5, CISCO fails to disclose "a second

switch blade" and "a third multiserver platform." Additionally, nowhere in CISCO is there any mention of "a central switch." While discussing claims 3 and 7, the Examiner states in the Final Office Action that "[s]ee page 9, Figure 9, the central switch is middle top switch on FDDI ring and is connected through FDDI ring to the bottom left (first blade switch) and top left (second blade switch) switch." *See* Final Office Action, Page 6, Lines 11-14. However, the icon referred to by the Examiner in Figure 9 is a router, not a central switch as alleged by the Examiner. For example, CISCO's Figure 2 shows the same icon and labels it "Cisco Router." Additionally, CISCO's Figure 7 shows the same icon and labels it "Cisco 7000." The product overview for the Cisco 7000 router is attached as Evidence Exhibit 5. The Applicant submits that a router is different than a central switch. Thus, CISCO fails to disclose "a central switch" as recited in Applicant's dependent claims 2 and 6.

Accordingly, the Applicant submits that claims 2 and 6 are allowable over the reference cited in the Final Office Action at least for the above reasons. The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 2 and 6.

D. Rejection of Dependent Claims 3 and 7

Claims 3 and 7 depend on dependent claims 2 and 6, respectively; which depend from independent claims 1 and 5, respectively. Therefore, the Applicant submits that

claims 3 and 7 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claims 1, 2, 5 and 6.

Accordingly, the Applicant submits that claims 3 and 7 are allowable over the reference cited in the Final Office Action at least for the above reasons. The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 3 and 7.

E. Rejection of Dependent Claims 4 and 8

Claims 4 and 8 depend on independent claims 1 and 5, respectively. Therefore, the Applicant submits that claims 4 and 8 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claims 1 and 5.

Accordingly, the Applicant submits that claims 4 and 8 are allowable over the reference cited in the Final Office Action at least for the above reasons. The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 4 and 8.

F. Rejection of Independent Claim 9

The Applicant turns to the rejection of claim 9 under 35 U.S.C. § 102(b) as being anticipated by CISCO. The Applicant submits that CISCO does not disclose or suggest at least the limitation of "**a first multiserver platform** comprising at least one of **a**

network interface and **a first switch blade**; and at least **a second multiserver platform** comprising **a second switch blade** coupled to said first switch blade of said first multiserver platform," as recited by the Applicant in the independent claim 9 (emphasis added).

With regard to "a first multiserver platform comprising at least one of a network interface and a first switch blade," the Final Office Action states the following:

> [A] first multiserver platform (for this claim, Page 8, Figure 8, right hand side block will be used for claim elements; bottom row) comprising at least one of a network interface (multiserver platform first one in bottom row, under VLAN1 and a network interface connecting to the switch to the multiserver) and a first switch blade (bottom block of three switches, second one connected to first multiserver platform under the label VLAN1).

See Final Office Action, Page 7, Lines 9-16. As mentioned above with regard to claims 1 and 5, nowhere in CISCO is a multiserver platform disclosed. CISCO's VLAN1 in Figure 8 is different than a multiserver platform. A multiserver platform is disclosed in Applicant's specification in, for example, at least Figure 1 and accompanying text in paragraphs 22-28. Further, neither Figure 8 nor the supporting text in CISCO mentions a network interface. CISCO discloses workstations connected to switches; however, because none of the workstations are shown directly connected to the network, CISCO can not disclose a workstation comprising a network interface, let alone a multiserver platform comprising a network interface. *See* CISCO, Figure 8, right hand side. Additionally, as mentioned above with regard to claims 1 and 5, nowhere in the CISCO reference is there any mention of using switch blades or server blades. Rather, the

CISCO reference discloses using the Catalyst 5000 and ProStack switches, which are not switch blades. *See* Evidence Exhibits 2 and 4.

Also, Applicant's claim 9 recites "a first multiserver platform **comprising** at least one of a network interface and a first switch blade." The Examiner asserts that the VLAN1 workstation in the bottom row of the right hand block in Figure 8 is a first multiserver platform (which it is not) and that it is **connected to** the ProStack switch in the bottom row of the right hand block in Figure 8. Thus, even if the workstation was a first multiserver platform (which it is not), CISCO fails to show the workstation **comprising** at least one of a network interface and a first switch blade. Rather, CISCO's Figure 8 shows the workstation **connected to** the switch. Nowhere in CISCO is there any disclosure that the VLAN workstations **comprise** at least one of a network interface and a first switch blade.

With regard to "at least a second multiserver platform comprising a second switch blade coupled to said first switch blade of said first multiserver platform," the Final Office Action states the following:

> [A]t least a second multiserver platform (second row) comprising a second switch blade (middle switch) coupled [to] said first switch blade of said first multiserver platform (middle switch connected to second multiserver platform, under the label VLAN1; both first multiserver platform and second multiserver platform are coupled by VLAN1).

See Final Office Action, Page 7, Line 16 - Page 8, Line 2. However, as mentioned above, nowhere in CISCO is a multiserver platform disclosed. CISCO's VLAN1 in Figure 8 is different than a multiserver platform. A multiserver platform is disclosed in

Applicant's specification in, for example, at least Figure 1 and accompanying text in paragraphs 22-28. Further, as mentioned above, nowhere in the CISCO reference is there any mention of using switch blades. Rather, the CISCO reference discloses using the Catalyst 5000 and ProStack switches, which are not switch blades. *See* Evidence Exhibits 2 and 4.

Additionally, Applicant's claim 9 recites "at least a second multiserver platform **comprising** a second switch blade coupled to said first switch blade of said first multiserver platform." The Examiner asserts that CISCO discloses "at least a second multiserver platform (second row) comprising a second switch blade (middle switch)...." *See* Final Office Action, Page 7, Lines 16-18. However, the CISCO's VLAN1 workstation in the second row of the right hand block in Figure 8 is shown as being **connected to** the Catalyst 5000 switch in the middle row of the right hand block in Figure 8. Thus, even if the workstation was a second multiserver platform (which it is not), CISCO fails to show the workstation **comprising** a second switch blade. Rather, CISCO's Figure 8 shows the workstation **connected to** the switch. Nowhere in CISCO is there any disclosure that the VLAN workstations **comprise** a second switch blade.

Accordingly, independent claim 9 is not anticipated by CISCO and is allowable. Furthermore, the Applicant reserves the right to argue additional reasons beyond those set forth herein td support the allowability of claim 9.

G. Examiner's Response to Arguments

The Examiner states the following in the Final Office Action:

> Examiner notes that switch blade is a device that performs switching functions (normally at layer 2 of the OSI model). ... As such the switches in Cisco document meet the functions performed by the Applicant's claimed switch blades.

See Final Office Action, Page 2, Lines 10-11 and 13-15. The Applicant points out that with regard to the anticipation rejections, MPEP 2131 states, "[a] claim is anticipated only if **each and every element as set forth in the claim is found**, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 2 USPQ2d 1051, 1053 (Fed.Cir. 1987) (emphasis added). MPEP 2131 also states, **"[t]he identical invention must be shown in as complete detail as is contained in the ... claim**." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

The Examiner does not contest that CISCO is silent as to a switch blade. Rather, the Examiner asserts that "the switches in Cisco document meet the functions performed by the Applicant's claimed switch blades." However, Applicant's independent claim 9 is a system claim; and therefore, components of Applicant's system are claimed and CISCO fails to disclose the claimed components of the system. Clearly, CISCO fails to disclose each and every element as set forth in Applicant's independent claim 9, as required by MPEP 2131 because CISCO at least fails to disclose "a first switch blade" and "a second switch blade." Further, CISCO fails to teach the identical invention in as complete detail as is contained in independent claim 9, as required by

MPEP 2131 because CISCO at least fails to disclose “a first switch blade” and “a second switch blade.”

Further, the Applicant notes that “switch blade” is a known term in the art. As already stated above, CISCO does not disclose the use of a “switch blade.” Even a broad interpretation of CISCO cannot overcome at least this deficiency.

With regard to “a multiserver platform,” the Applicant notes that the Examiner’s Response to Arguments section of the Final Office Action merely discusses CISCO’s disclosure of using more than one server. However, the use of more than one server does not necessarily mean using a multiserver platform. For example, the Applicant’s specification discusses the disadvantages of using multiple single servers in at least paragraphs [06] and [07]. Nowhere in CISCO is there any mention of using multiserver platforms. Thus, CISCO clearly fails to disclose each and every element as set forth in Applicant’s independent claim 9, as required by MPEP 2131 because CISCO at least fails to disclose “a first multiserver platform” and “a second multiserver platform.” Further, CISCO fails to teach the identical invention in as complete detail as is contained in independent claim 9, as required by MPEP 2131 because CISCO at least fails to disclose “a first multiserver platform” and “a second multiserver platform.”

Further, the Applicant notes that “multiserver platform” is a known term in the art. As already stated above, CISCO does not disclose the use of a “multiserver platform.” Even a broad interpretation of CISCO cannot overcome at least this deficiency.

H. Rejection of Dependent Claim 10

Claim 10 depends on independent claim 9. Therefore, the Applicant submits that claim 10 is allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 9.

Accordingly, the Applicant submits that claim 10 is allowable over the reference cited in the Final Office Action at least for the above reasons. The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claim 10.

I. Rejection of Dependent Claim 11

Claim 11 depends on dependent claim 10, which depends on independent claim 9. Therefore, the Applicant submits that claim 11 is allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claims 9 and 10.

Accordingly, the Applicant submits that claim 11 is allowable over the reference cited in the Final Office Action at least for the above reasons. The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claim 11.

J. Rejection of Dependent Claim 12

Claim 12 depends on dependent claim 10, which depends on independent claim 9. Therefore, the Applicant submits that claim 12 is allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claims 9 and 10.

Accordingly, the Applicant submits that claim 12 is allowable over the reference cited in the Final Office Action at least for the above reasons. The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claim 12.

K. Rejection of Dependent Claim 13

Claim 13 depends on independent claim 9. Therefore, the Applicant submits that claim 13 is allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 9. The Applicant also submits that CISCO does not disclose or suggest at least the limitation of "further comprising at least one central switch coupled to at least said first switch blade of said first multiserver platform and said second switch blade of said second multiserver platform," as recited by the Applicant in claim 13.

With regard to claim 13, the Final Office Action states that CISCO discloses "further comprising at least one central switch (page 9, Figure 9, top central switch). *See* Final Office Action, Page 10, Lines 6-8. However, nowhere in CISCO is there any

mention of "a central switch." Rather, the icon referred to by the Examiner in Figure 9 is a router, not a central switch as alleged by the Examiner. For example, CISCO's Figure 2 shows the same icon and labels it "Cisco Router." Additionally, CISCO's Figure 7 shows the same icon and labels it "Cisco 7000." The product overview for the Cisco 7000 router is attached as Evidence Exhibit 5. The Applicant submits that a router is different than a central switch. Thus, CISCO fails to disclose "a central switch" as recited in Applicant's dependent claim 13.

The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claim 13.

L. Rejection of Dependent Claim 14

Claim 14 depends on dependent claim 13, which depends on independent claim 9. Therefore, the Applicant submits that claim 14 is allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claims 9 and 13.

The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claim 14.

M. Rejection of Dependent Claim 15

Claim 15 depends on dependent claim 14, which depends on dependent claim 13, which depends on independent claim 9. Therefore, the Applicant submits that claim 15 is allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claims 9, 13 and 14.

The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claim 15.

CONCLUSION

For at least the foregoing reasons, the Applicant submits that claims 1-15 are in condition for allowance. Reversal of the Examiner's rejection and issuance of a patent on the application are therefore requested.

The Commissioner is hereby authorized to charge $510 (to cover the Brief on Appeal Fee) and any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Respectfully submitted,

Date: 16-JUNE-2008

By: /Philip Henry Sheridan/
Philip Henry Sheridan
Reg. No. 59,918
Attorney for Applicant

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
(T) 312 775 8000
(F) 312 775 8100

(PHS)

CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

1. A method for communication information in a server platform, the method comprising:

receiving at least one packet from at least one of a first switch blade associated with a first multiserver platform;

determining at least a server blade associated with a second multiserver platform for receiving at least a portion of said received at least one packet; and

routing said at least a portion of said at least one received packet to at least said server blade.

2. The method according to claim 1, wherein said receiving further comprises receiving said at least one packet by at least one of a second switch blade associated with a third multiserver platform and a central switch.

3. The method according to claim 2, further comprising if said at least one packet is received by said central switch, communicating said at least a portion of said at least one received packet to at least a third switch blade associated with said second multiserver platform via at least one communication link that couples said central switch directly to said at least said third switch blade.

4. The method according to claim 1, further comprising processing said routed at least a portion of said at least one received packet by said at least said server blade.

5. A machine-readable storage having stored thereon, a computer program having at least one code section for communicating information in a server platform, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

receiving at least one packet from at least one of a first switch blade associated with a first multiserver platform;

determining at least a server blade associated with a second multiserver platform for receiving at least a portion of said received at least one packet; and

routing said at least a portion of said at least one received packet to at least said server blade.

6. The machine-readable storage according to claim 5, further comprising code for receiving said at least one packet by at least one of a second switch blade associated with a third multiserver platform and a central switch.

7. The machine-readable storage according to claim 6, further comprising code for communicating said at least a portion of said at least one received packet to at least a third switch blade associated with said second multiserver platform via at least

one communication link that couples said central switch directly to said at least said third switch blade, if said at least one packet is received by said central switch.

8. The machine-readable storage according to claim 5, further comprising code for processing said routed at least a portion of said at least one received packet by said at least said server blade.

9. A system for communicating information in a server platform, the system comprising:

a first multiserver platform comprising at least one of a network interface and a first switch blade; and

at least a second multiserver platform comprising a second switch blade coupled to said first switch blade of said first multiserver platform.

10. The system according to claim 9, further comprising at least a third multiserver platform comprising a third switch blade coupled to at least one of said second switch blade of said second multiserver platform and said first switch blade of said first multiserver platform.

11. The system according to claim 10, wherein said first multiserver platform, said second multiserver platform and said third multiserver are coupled in a daisy-chain configuration.

12. The system according to claim 10, wherein said first multiserver platform, and said third multiserver platform communicate via said second multiserver platform.

13. The system according to claim 9, further comprising at least one central switch coupled to at least said first switch blade of said first multiserver platform and said second switch blade of said second multiserver platform.

14. A system according to claim 13, further comprising at least a third switch blade of a third multiserver platform coupled to said at least one central switch.

15. The system according to claim 14, wherein said first multiserver platform, said second multiserver platform and said third multiserver platform communicate via said central switch.

EVIDENCE APPENDIX

(37 C.F.R. § 41.37(c)(1)(ix))

(1) CISCO Systems, Virtual LAN Communications, http:/./web.archive.org/web/19990209172148/cio.cisco.com/warp/public/614/13.html, July 14, 1995 ("CISCO"), entered into record by Examiner Hari P. Kunamneni in the March 27, 2007 Office Action.

(2) CISCO Systems, Catalyst 5000 Family Installation Guide, Chapter 1, Product Overview, Chapter 4, Installing the Switch, http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/hardware/installg/01intro.pdf and http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/hardware/installg/04instal.pdf, May 2000 ("Evidence Exhibit 2").

(3) CISCO Systems, Catalyst 1200 Installation and Configuration Guide, Chapter 1, Product Overview, Chapter 3, Hardware Installation, http://www.cisco.com/univercd/cc/td/doc/product/lan/catalyst/cat12icg/61644.pdf and http://www.cisco.com/univercd/cc/td/doc/product/lan/catalyst/cat12icg/61637.pdf, 1989-1997 ("Evidence Exhibit 3").

(4) KMJ Communications, Kalpana ProStack System, Product Overview, http://www.kmj.com/kalpana/kpro.html and Business Wire, Kalpana ProStack Delivers New Stackable Architecture For Ethernet Switching,

http://findarticles.com/p/articles/mi_m0EIN/is_1995_March_28/ai_16719320/print, March 28,1995 ("Evidence Exhibit 4").

(5) CISCO Systems, Cisco 7000 User Guide, Chapter 1, Product Overview, http://www.cisco.com/univercd/cc/td/doc/product/core/cis7000/7000ug/prodo0ug.pdf, October 19, 2001 ("Evidence Exhibit 5").

RELATED PROCEEDINGS APPENDIX
(37 C.F.R. § 41.37(c)(1)(x))

The Appellant is unaware of any related appeals or interferences.

Virtual LAN Communications

- **Statement of Direction: Cisco VLAN Roadmap**
- **White Paper: Cisco IOS VLAN Services**
- **Technology Brief: VLAN Interoperability**

Introduction

Today's cost-effective, high-performance **local-area network (LAN) switches** offer users superior microsegmentation, low-latency packet forwarding, and increased bandwidth across the corporate backbone. LAN switches also can segment networks into logically defined virtual workgroups. This logical segmentation, commonly referred to as virtual LAN (VLAN) communication, offers a fundamental change in how LANs are designed, administered, and managed. While logical segmentation provides substantial benefits in LAN admini-stration, security, and management of network broadcast activity across the enterprise, there are many components of VLAN solutions that must be considered prior to large scale VLAN deployment.

These additional VLAN components include high-performance switches that logically segment connected end stations, transport protocols that carry VLAN traffic across shared LAN and **Asynchronous Transfer Mode (ATM)** backbones, layer 3 routing solutions that extend VLAN communications between **workgroups**, system compatibility and **interoperability** with previously installed LAN systems, and network management solutions that offer centralized control, configuration, and traffic management functions. Figure 1 summarizes these concepts. All of these components are critical for enterprise-wide VLAN solutions, because they provide the scalability necessary for migrating from an installed base of shared LAN technologies to the new, emerging architecture of per-user switched communications.

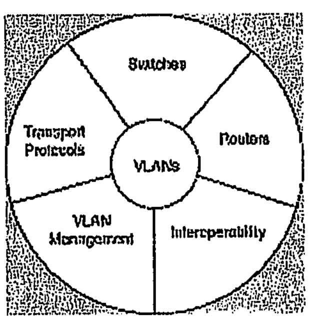


Figure 1: VLAN System Components

The first section of this document briefly discusses the importance of each one of these components within VLAN architectures. The second section reviews the benefits of VLANs and their applicability

within workgroups and across the enterprise backbone.

Building VLAN Solutions

Removing the Physical Boundaries

Conceptually, VLANs provide greater segmentation and organizational flexibility. VLAN technology allows network managers to group switch ports and users connected to them into logically defined communities of interest. These groupings can be coworkers within the same department, a cross-functional product team, or diverse users sharing the same network application or software (such as Lotus Notes users). Grouping these ports and users into communities of interest, referred to as VLAN organizations, can be accomplished within a single switch, or more powerfully, between connected switches within the enterprise. By grouping ports and users together across multiple switches, VLANs can span single building infrastructures, interconnected buildings, or even wide-area networks (WANs). VLANs completely remove the physical constraints of workgroup communications across the enterprise, as shown in Figure 2.

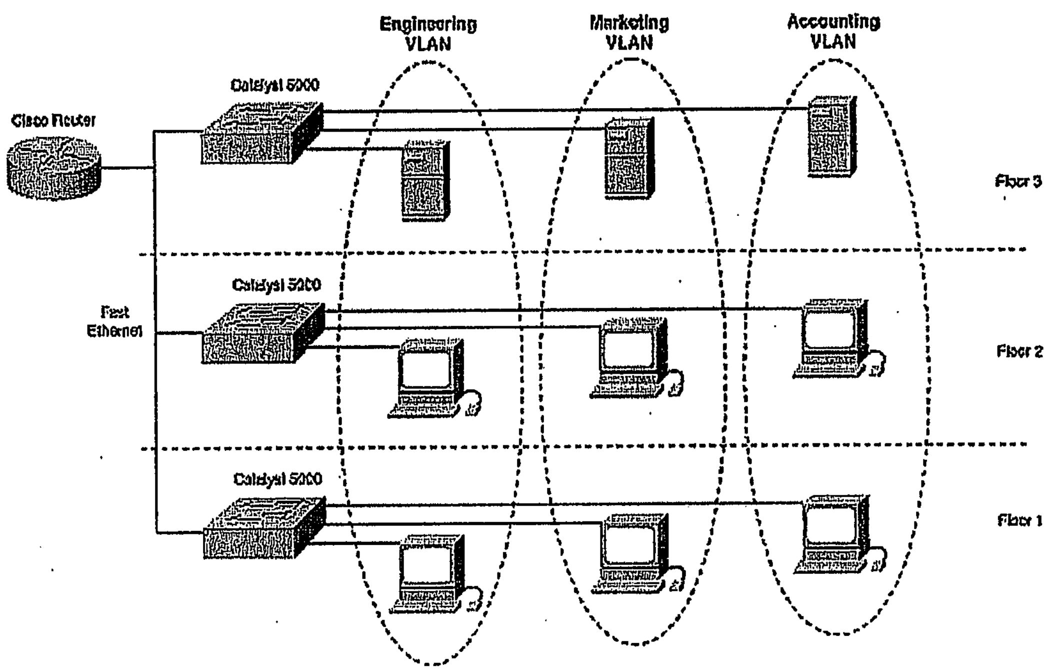


Figure 2: Logically Defined Networks (VLANs)

VLANs provide the ability for any organization to be physically dispersed throughout the company while maintaining its group identity. For example, accounting personnel can be located on the shop floor, in the research and development center, in the cash disbursement office, and in the corporate offices, while at the same time all members reside on the same virtual network, sharing traffic only with each other. Figure 3 illustrates a typical VLAN architecture that places these employees closer to their assigned areas of management and the people with whom they interact, while maintaining communication integrity within their respective organization.

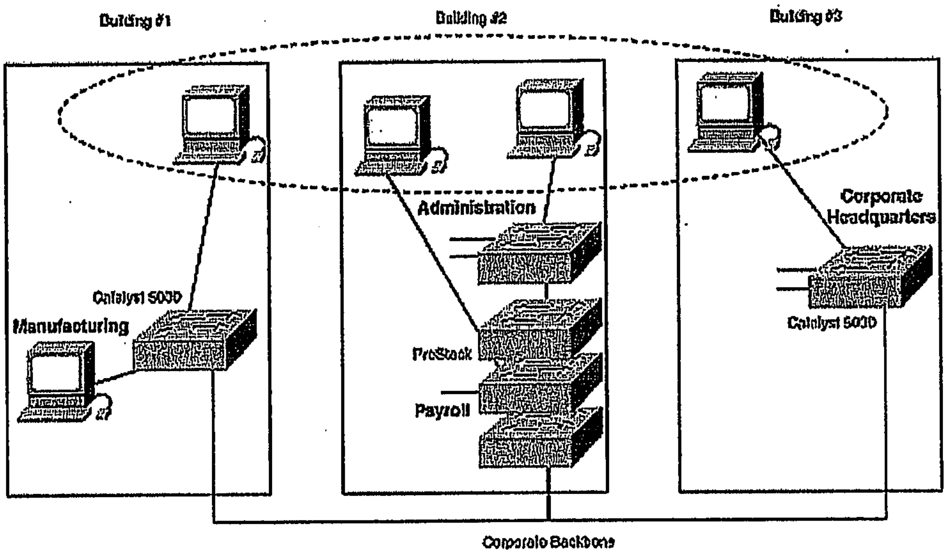


Figure 3: Logical Communication Between Users

Today's VLANs better match the way that companies are organized, and allow network managers to more closely align the network to the way that employees work and communicate.

Switches -- the Core of VLANs

Switches are one of the core components of VLAN communi-cations. They are the entry point for end-station devices into the switched fabric and for communication across the enterprise. Switches provide the intelligence to group users, ports, or logical addresses into common communities of interest. Each switch has the intelligence to make filtering and forwarding decisions by packet, based on VLAN metrics defined by network managers, and to communicate this information to other switches and routers within the network. And while today LAN switches are installed between shared segment hubs and routers located within the backbone, they will take on a larger, more significant role for VLAN segmentation and low-latency forwarding as they are deployed in the wiring closet. LAN switches offer significant increases in performance and dedicated bandwidth across the network, with the intelligence necessary for VLAN segmentation.

The most common approaches for logically grouping users into administratively defined VLANs include *packet filtering* and *packet identification*. Packet filtering is a technique that examines particular information about each packet based on user-defined offsets. Packet identification (tagging) uniquely assigns a user-defined ID to each packet. Both of these techniques examine the packet when it is either received or forwarded by the switch. Based on the set of rules defined by the administrator, these techniques determine where the packet is to be sent, filtered, and/or broadcast. These control mechanisms can be centrally administered (with network management software) yet are easily deployed throughout the network.

The concepts of packet filtering are very similar to those commonly used for routers. A filtering table is developed for each switch. This provides a high level of administrative control, because it can examine many attributes of each packet. Network managers can group users based upon MAC station addresses, network layer protocol types, and/or application types. Table entries are compared with the packets filtered by the switch. The switch takes the appropriate action based on the entries (see Figure 4).

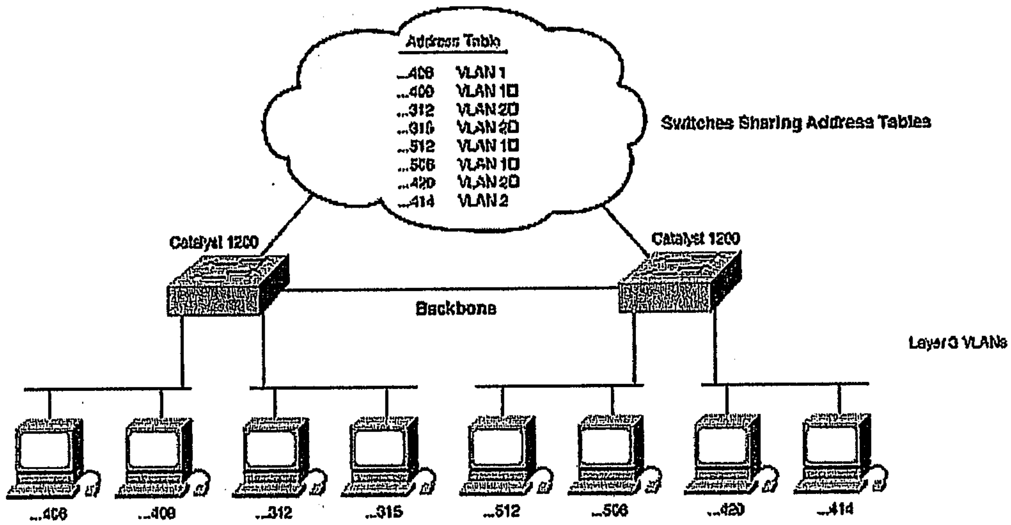


Figure 4: Packet Filtering

Packet filtering typically provides an additional layer of switch processing prior to forwarding each packet to another port or switch within the network, and it becomes more apparent as you filter deeper into each packet. This additional processing can effect switch latency and overall network performance. In addition, maintaining address tables adds an extra layer of administration per switch and requires synchronizing tables between switches.

VLAN packet identification (packet tagging) is a relatively new approach that has been specifically developed for switched communications. This approach places a unique identifier in the header of each packet as it is forwarded throughout the switch fabric. The identifier is understood and examined by each switch prior to any broadcasts or transmissions to other switches, routers, or end-station devices. When the packet exits the switch fabric, the switch removes the identifier before the packet is transmitted to the target end station. Over the past two years, packet identification has gained acceptance as switches have increased in popularity; packet identification functions at layer 2 and requires little processing or administrative overhead (see Figure 5).

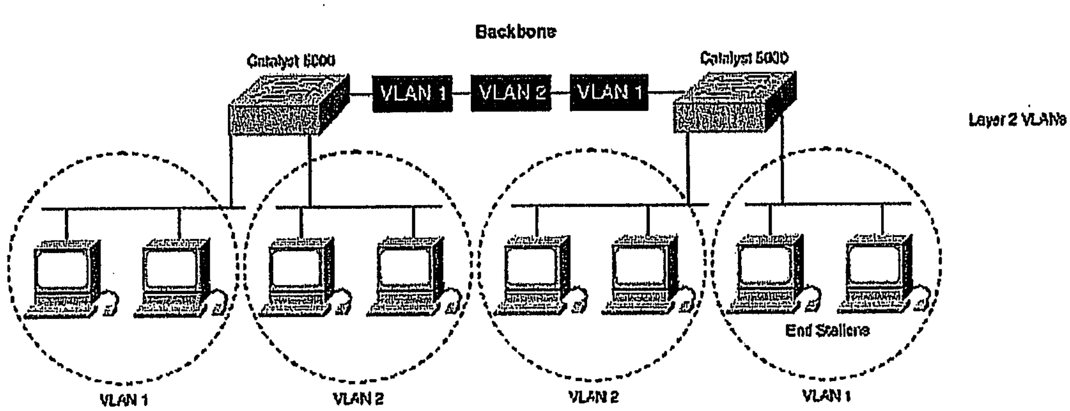


Figure 5: Packet Identification

The overall benefits of both approaches (packet filtering and packet identification) allow VLAN architectures that are nonintrusive to end-node applications and communication protocols. Switches provide all of the filtering, identification, and forwarding without any modification to the attached end station devices. This delivers a VLAN architecture that easily integrates with existing LAN applications while offering scalability and migration to ATM networks.

Configuring VLANs

Users can be assigned to VLANs using several different configuration options that include static port assignments, dynamic port assignments, and multi-VLAN port assignments. These options are a function of the switch's capabilities (as mentioned in the previous section), the manner in which the stations are attached to each port on the switch, and the capabilities of the VLAN management software.

Stations directly attached to the ports on the switch provide the greatest flexibility for VLAN configuration and management. All stations can be uniquely assigned to VLANs. When they move to other physical locations using other directly attached switch port connections, they maintain their VLAN identities irrespective of their new locations. Stations connected to a switch through a shared hub are commonly grouped within the same VLAN because they all share the same switch port. While this approach is less flexible for each user on the network, it still provides highly desirable VLAN solutions for network managers. Additionally, hubs that provide multibackplane connection options increase the flexibility for unique VLAN assignments. Each backplane connection from the hub to a switch port can be individually assigned to a VLAN.

Static VLANs are ports on a switch that a network manager has statically assigned to a VLAN, using either a VLAN management application or has configured directly within the switch. These ports maintain their assigned VLAN configurations until the network manager takes another action. Although static VLANs require changes by the network operator, they are secure, easy to configure, and straightforward to monitor. These type of VLANs work well in networks where network moves are controlled and managed, where there is robust VLAN management software to configure the ports, and where network managers do not want to take on the additional overhead of maintaining end-station MAC addresses and custom filtering tables.

Dynamic VLANs are ports on a switch that can automatically determine their VLAN assignments with the aid of intelligent management software. Dynamic VLANs function based on their assignments to end-user station MAC addresses, logical addresses, or protocol type. These assignments are entered and maintained in a centralized VLAN management application. When a station is initially connected to an unassigned switch port, the appropriate switch checks the MAC address entry in the VLAN management database and dynamically configures the port with the corresponding VLAN configuration. The major benefits of this approach are less administration within the wiring closet when a user is added or moved, and centralized notification when an unrecognized user is added to the network. Typically, more administration is required up front to set up the database within the VLAN management software and to maintain an accurate database of all network users, as shown in Figure 6.

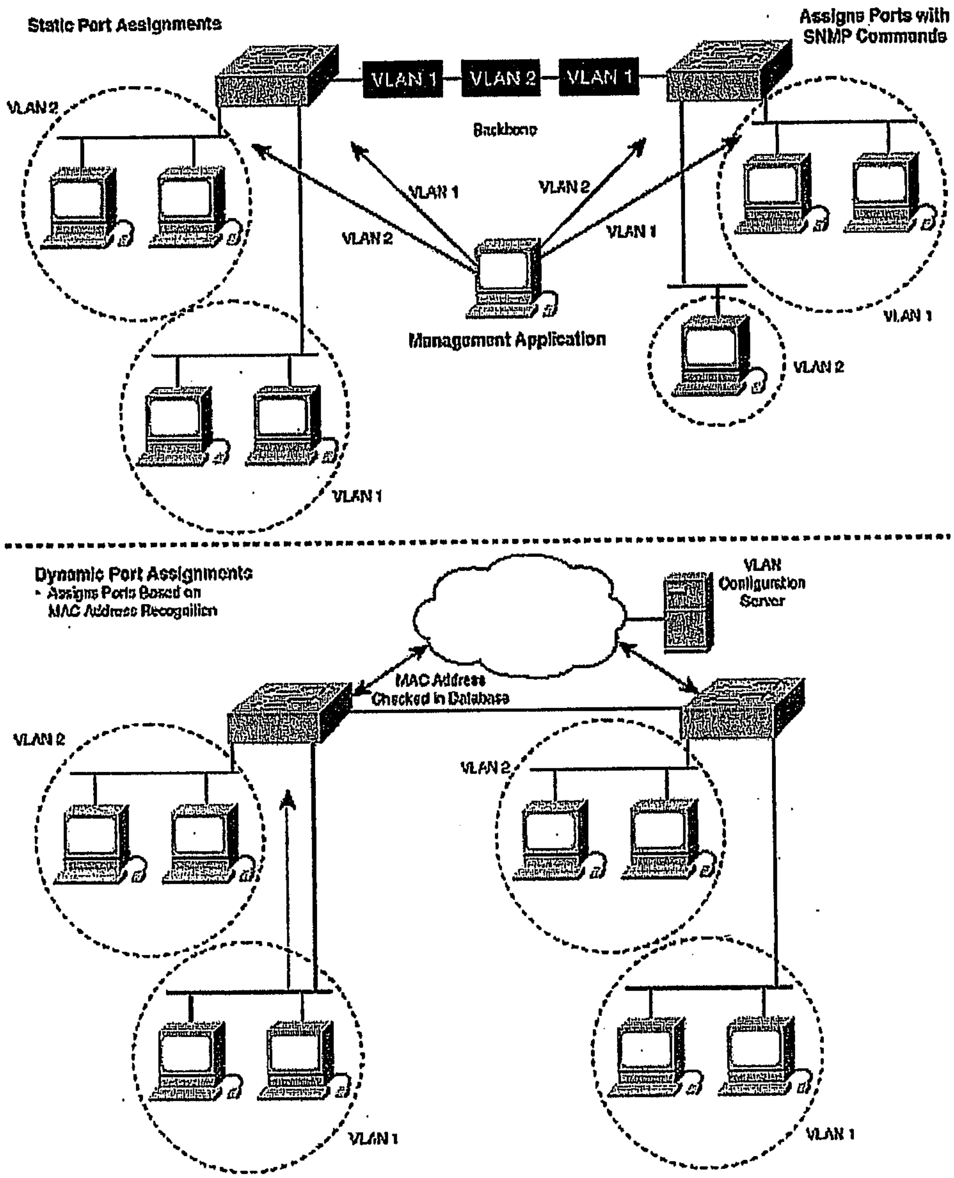


Figure 6: Configuring Ports to VLANs

Multi-VLAN port configurations provide communications among multiple VLANs concurrently either from a single port or a single user. This includes shared servers and users who need to belong to multiple workgroups. While there are several solutions on the market today that provide this functionality, there is an associated tradeoff. Concurrent port sharing across multiple groups dramatically reduces the firewalls between workgroups and the security these firewalls provide. These ports act as gateways into other VLAN groups and, in effect, create one larger VLAN. This approach does not scale well as the intersection between these VLAN groups becomes larger and larger.

For resources that need to participate in several VLANs concurrently, a better approach is to attach the end station directly to the backbone and to configure unique communication paths to each individual VLAN, thus providing resource sharing while maintaining the integrity of the VLAN firewalls. This approach has been defined in the ATM LAN Emulation draft standards and is also being evaluated for

implementation across shared-LAN backbones and switching architectures, illustrated by Figure 7.

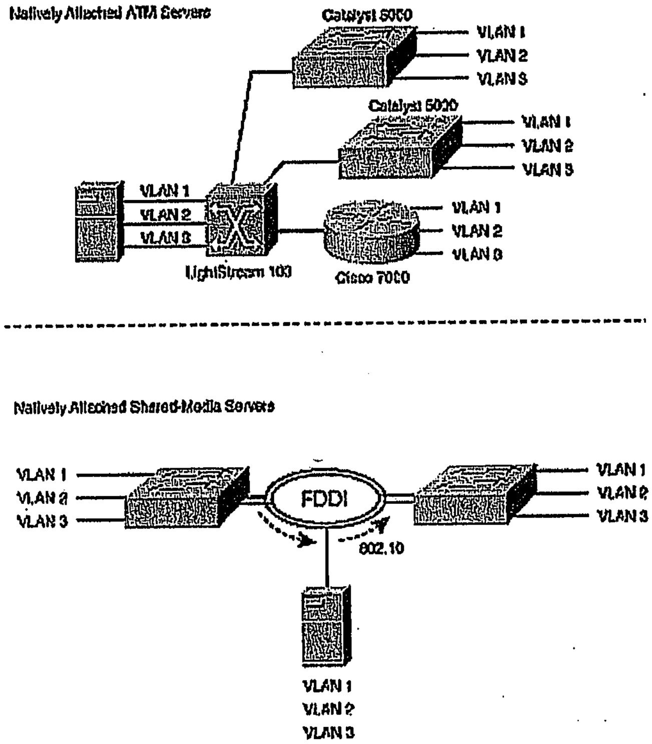


Figure 7: Servers as Part of Multiple VLANs

Segmenting with Switching Architectures

Restructuring users according to logical associations across the enterprise rather than physical location is a fundamental shift away from the topologies deployed today. A large majority of networks currently installed provide very limited logical segmentation. Users are commonly grouped based on their connections into the shared hub and the router ports between these hubs. In addition, users on two different hubs segmented with a router cannot be connected to the same LAN segment. This topology provides segmentation only between the hubs, which are typically located on separate floors, and not between users connected to the same hub. It imposes physical constraints on the network and greatly limits the manner in which users can be grouped. And while some shared hub architectures provide a small degree of grouping capabilities, network managers are restricted in the way they can configure logically defined workgroups.

Switches remove the physical constraints imposed by a shared-hub architecture because they logically group users and ports across the enterprise. As a replacement for shared hubs, switches remove the physical barriers imposed within each wiring closet. Additionally, the role of the router evolves beyond the more traditional role of firewalls and broadcast suppression to policy-based control, broadcast management, and route processing and distribution. Equally as important, routers remain vital for switched architectures configured as VLANs because they provide the communication between logically defined workgroups (VLANs). Routers also provide VLAN access to shared resources such as servers and hosts, and connect to other parts of the network that are either logically segmented with the more traditional subnet approach or require access to remote sites across wide-area links. Layer 3

communication, either embedded in the switch or provided externally, is an integral part of any high-performance switching architecture.

External routers can be cost-effectively integrated into the switching architecture using one or multiple high-speed backbone connections. These are typically FDDI, Fast Ethernet, or ATM-type connections. These connections increase the throughput between switches and routers, provide a one-to-one logical association between the configured VLANs and layer 3 subnets, and consolidate the overall number of physical router ports required for communication between VLANs. As illustrated in Figure 8, this architecture not only provides logical segmentation, it greatly enhances the efficiency of the network.

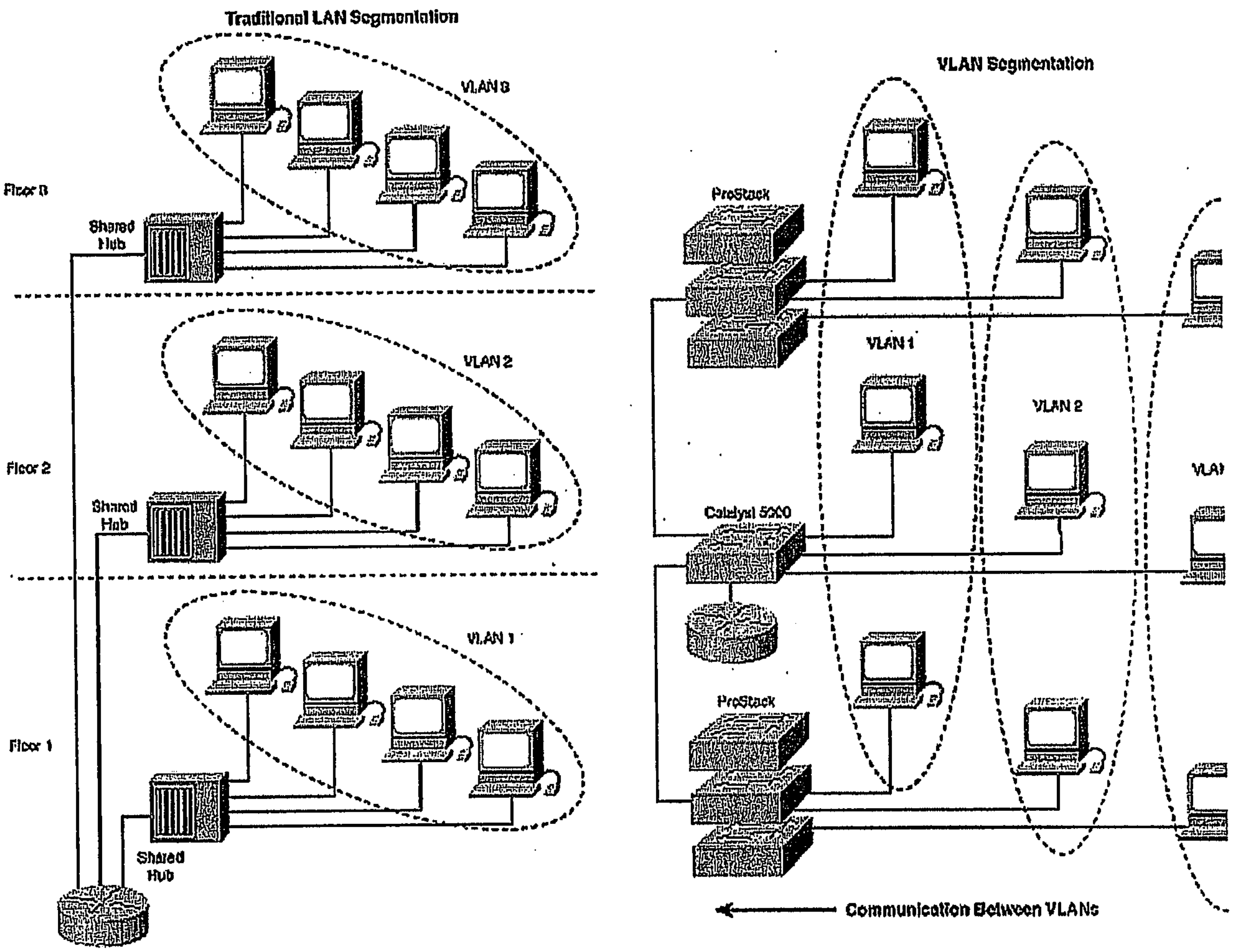


Figure 8: Topology Changes of VLANs

VLANs across the Backbone

Important to any VLAN architecture is the ability to transport VLAN information between interconnected switches and routers that reside on the corporate backbone. It is the VLAN transport that enables enterprisewide VLAN communications. These transport capabilities remove the physical boundaries between users, increase the configuration flexibility of a VLAN solution when users move, and provide mechanisms for interoperability between backbone system components.

The backbone commonly acts as the aggregation point for large volumes of traffic. It also carries end-user VLAN information and identification between switches, routers, and directly attached servers. Within the backbone, high-bandwidth, high-capacity links are typically chosen to carry the traffic throughout the enterprise. The three most popular high bandwidth options include Fast Ethernet, Fiber Distributed Data Interface (FDDI), Copper Distributed Data Interface (CDDI), and ATM. Because switches and routers directly attach to the backbone, they must be able to transport VLAN information and interoperate with other network components.

In response to these requirements, several different transport mechanisms are being considered for communicating VLAN information across high-performance backbones. Among them is the LAN Emulation draft standard that has recently been approved by the ATM Forum and the IEEE 802.10 protocol which provides VLAN communication across shared backbones. Both of these define an interoperable mechanism for configuring and transporting VLANs across different backbone technologies.

The 802.10 proposal has been recommended by switching, routing, and hub vendors. Figure 9 shows typical applications for 802.10. This proposal defines a 32-bit addressing scheme within an 802.10 packet for VLAN identification, an addressing scheme nonintrusive to existing backbone architectures; however, it requires that switches include built-in software intelligence for enterprise VLAN communications. With the standardization of these two transport protocols, network managers can implement VLANs within individual workgroups, across the enterprise backbone, and gain access to WANs. In addition, Cisco has developed the inter-switch link (ISL) VLAN transport protocol to deliver efficient communication across Fast Ethernet backbones. Cisco will implement this as a de-facto standard and has made the specification available to vendors who want to interoperate.

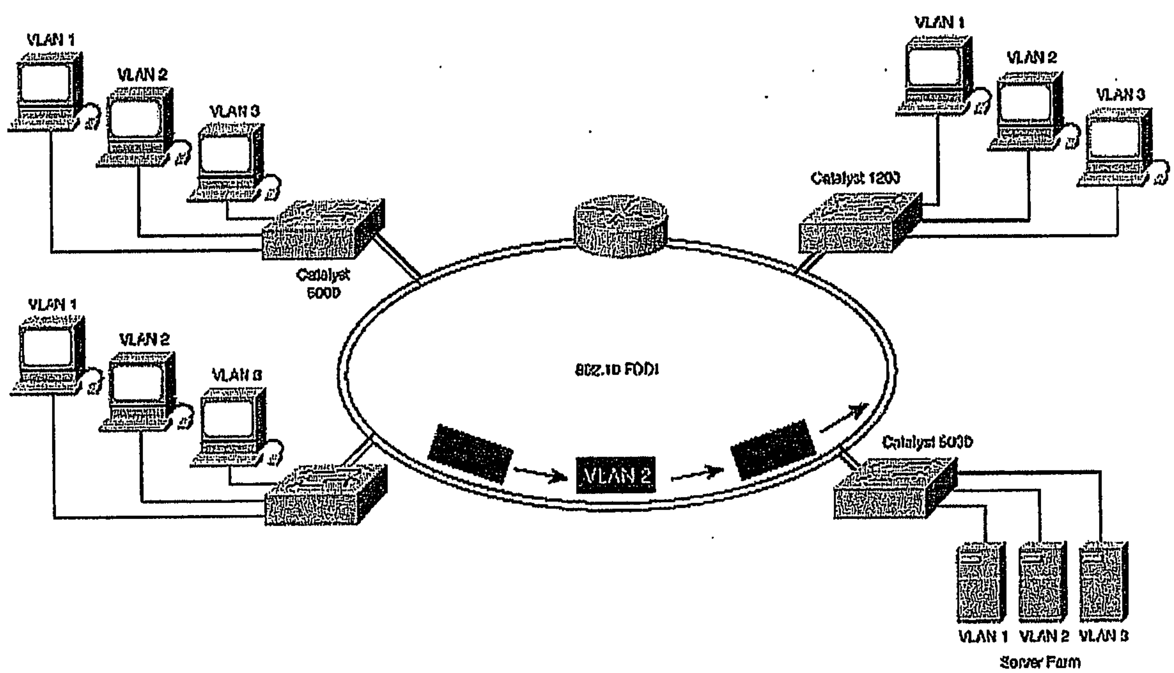


Figure 9: VLANs across FDDI Backbones

VLAN Integration

Traditional network architectures are experiencing significant changes as they evolve toward greater microsegmentation, more capacity across the backbone, and dedicated circuit switching with the adoption of ATM. At the core of these changes are LAN-based switches with wiring closet applications, backbone switches for greater throughput performance, and ATM switches for dedicated circuit switching. As network managers migrate to these products, VLANs become a reality. Typically, the integration of VLANs begins with the first switch installation in a department or building. As the number of switches grows throughout the enterprise, VLANs become an enterprisewide solution. These enterprisewide VLANs require the transport mechanism, management tools, and layer 3 communication for logical segmentation and access across the network.

VLANs become a natural inclusion for LAN architectures as network designers and managers seek dedicated bandwidth to the desktop and segmentation based upon logical workgroups across the enterprise. Switching architectures that are VLAN- capable, along with routing solutions that interconnect VLANs, are evolutionary design changes compared with the physical segmentation that a majority of networks have in place today. VLANs are one of the essential technologies for breaking today's restrictive paradigm.

The Benefits of VLANs

VLANs are often positioned as solving the problems associated with moves, adds, and changes. While they do reduce a large part of the administration costs when users change locations within a building or campus, VLAN technology provides many internetworking benefits that are equally as compelling. In addition to the reduced costs of administration, VLAN benefits include tighter network security with establishment of secure user groups, better management and control of broadcast activity, microsegmentation of the network without sacrificing scalability, load distribution of traffic across traffic-intensive switches ("hot spots" within the network), and the relocation of workgroup servers into secured, centralized locations.

Improved Administration Efficiencies

Companies continuously reorganize as they seek productivity improvements. On average, between 20 and 40 percent of the workforce is physically moved every year. These moves, adds, and changes are one of a network manager's biggest headaches and one the largest expenses relative to managing the network. Many moves require re-cabling, and almost all moves require new station addressing and hub and router reconfigurations. And, invariably, about the time managers stabilize their networks, more changes are requested.

VLANs provide an effective mechanism for controlling these changes and reducing much of the cost associated with hub and router reconfigurations. Users in a VLAN can share the same network "address space" regardless of their location. When users in a VLAN are moved from one location to another, as long as they remain within the same VLAN and are connected to a switch port, their network addresses do not change. Location changes can be as simple as plugging a user into a port on a VLAN-capable switch, or simply configuring the port on the switch to that VLAN, as shown in Figure 10. This greatly simplifies the rewiring, configuration, and debugging necessary to get the user back on line. It is a significant improvement over the techniques used within the wiring closet today. Moreover, router configuration remains intact; a simple move of a user from one location to another does not create any configuration modifications in the router as long as the user resides within the same VLAN.

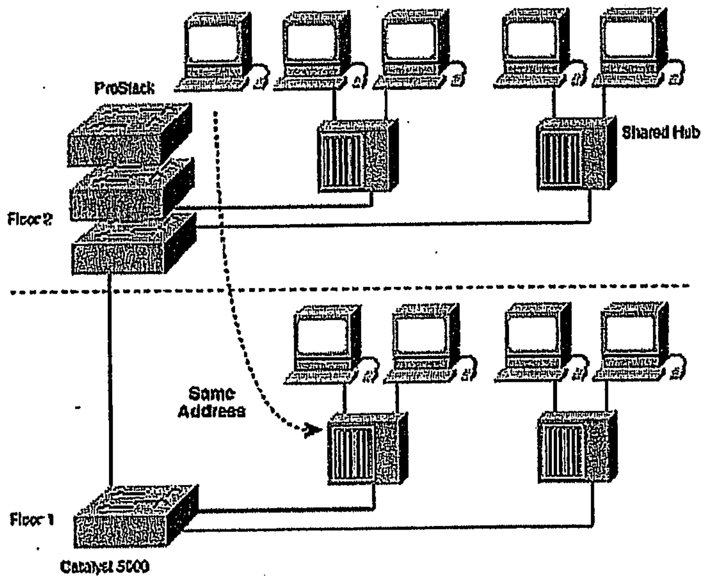


Figure 10: Controlling Broadcasts

Controlling Broadcast Activity

Broadcast traffic, whether it is controlled through effective segmentation or by pruning an application's behavior, occurs in every network. Broadcast frequency depends on the types of applications, the types of servers, the amount of logical segmentation, and how these network resources are used. While applications have been fine-tuned over the last few years to reduce the number of broadcasts they send out, new multimedia applications are being developed that are broadcast- and multicast-intensive. Operationally, broadcasts can occur as a result of faulty network interface cards and communication devices. If not properly managed, they can seriously degrade network performance and can potentially bring down an entire network. This type of failure is primarily due to inadequate firewalls, internetworking loops, faulty network devices, or broadcast-intensive applications.

Network managers must take preventive measures to ensure against broadcast-related problems. One of the most effective measures is to properly segment the network with protective firewalls that minimize problems on one segment from damaging other parts of the network. Thus while one segment may exhibit excessive broadcast conditions as a result of a faulty network device or a mismanaged application, the rest of the network is protected with a firewall, commonly provided by a router. Firewall segmentation provides reliability, safeguards the network from the inefficient use of bandwidth, and minimizes the overhead of broadcast traffic allowing for greater throughput of application traffic.

As many designers migrate their networks toward switching architectures, they begin to lose the firewalls and safeguards that routers provide. By not placing any routers between the switches, broadcasts (layer 2 transmissions) are sent to every switched port. This is commonly referred to as a "flat" network where there is one broadcast domain across the entire network. The advantage of a flat switched network is that it provides very low latency and high throughput performance; the disadvantage is that it increases the susceptibility to broadcast traffic across all switches, ports, backbone links, and users.

Similar to routers, VLANs offer an effective mechanism for setting up firewalls within a switch fabric

and protecting the network against potentially dangerous broadcast problems. Additionally, VLANs maintain all of the performance benefits of switching. These firewalls are accomplished by assigning switch ports, and/or users to specific VLAN groups both within single switches and across multiple connected switches. Broadcast traffic within one VLAN is not transmitted outside the VLAN. Conversely, adjacent ports do not receive any of the broadcast traffic generated from other VLANs. This type of configuration substantially reduces the overall broadcast traffic, frees bandwidth for real user traffic, and lowers the overall vulnerability of the network to broadcast storms (see Figure 11).

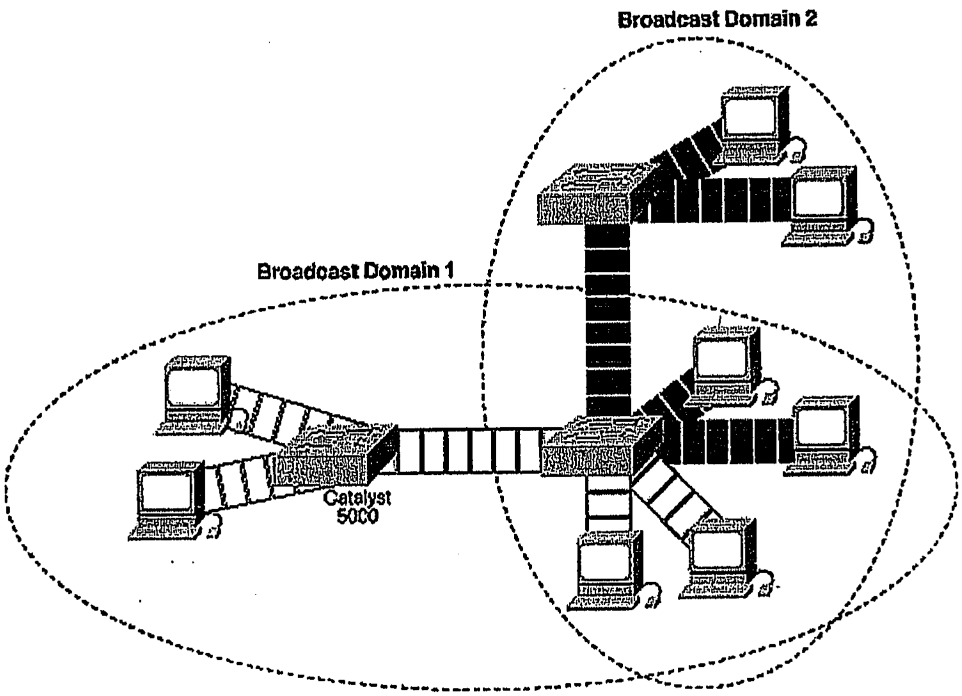


Figure 11: Added Security of Routers

Network managers can easily control the size of the broadcast domain by regulating the overall size of their VLANs, restricting the number of switch ports within a VLAN and the number of users residing on these ports. The smaller the VLAN group, the less effect broadcast traffic activity within the VLAN group has on everyone else within the network. Additionally, VLAN groups can be assigned based on the type of applications used and the amount of broadcasts these applications create. Users sharing an application that is very broadcast intensive are placed in the same VLAN group, while at the same time allowing the network manager to distribute the application across the campus.

Enhanced Network Security

Over the past five years the use of LANs has increased exponentially. As a result, LANs often have confidential, mission-critical data moving across them. Confidential data requires security through access restriction. One of the inherent shortcomings of shared LANs is that they are relatively easy to penetrate. By plugging into a live port, an intrusive user has access to all broadcasts within the segment. The larger the broadcast group, the greater the access unless there are security control functions in the hub.

One of the most cost effective and easiest administrative techniques to increase security is to segment

the network into distinct broadcast groups. Additionally, it allows the network manager to restrict the number of users in a VLAN group and to disallow another user from joining without first receiving approval from the VLAN network management application. VLANs thus provide security firewalls, restrict individual user access, flag any unwanted intrusion to a network manager, and control the size and composition of the group.

Implementing this type of segmentation is relatively straightforward. Switch ports are grouped together based on the type of applications and access privileges. Restricted applications and resources are commonly placed in a secured VLAN group. Any users trying to tap into these secured VLANs are flagged by the network management software. Further security enhancements can be added using router access lists. These are especially useful when communicating between VLANs. On the secured VLAN, the router restricts access into the group as configured on both the switches and the routers. Restrictions can be placed based on station addresses, application types, protocols types, or even by time of day (see Figure 12).

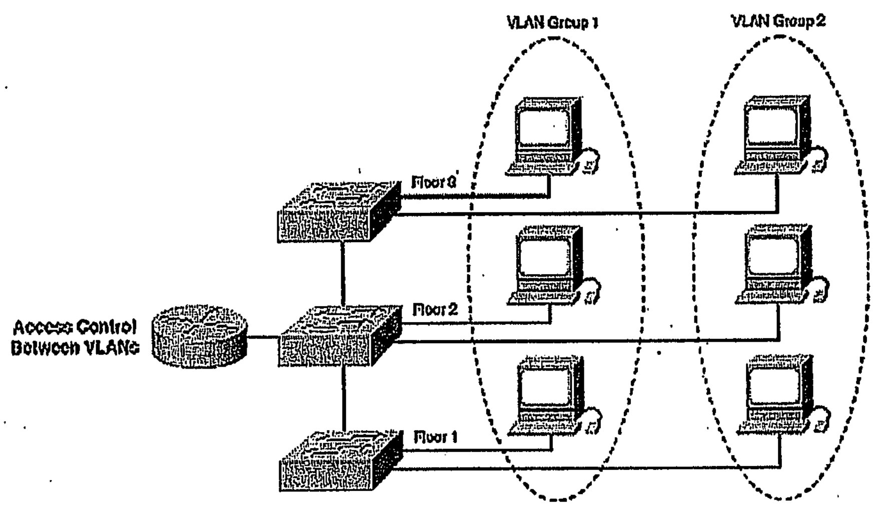


Figure 12: Simplification of Moves with VLANs

Leveraging Legacy Hub Investments

Over the last three to five years, network administrators have installed a significant number of shared hub chassis, modules, and stackable devices. While many of these devices are being replaced with newer switching technologies as network applications require more dedicated bandwidth and performance directly to the desktop, these concentrators still perform useful functions in many existing installations. Network managers are leveraging their investments by connecting switches to the backplanes of the hubs. In the context of this discussion, a backplane hub connection defines any shared-media hub connection into a network backbone; stackable hubs, hub chassis, and even hub modules provide some form of this connection. It is the connections between the shared hubs and the switches that provide opportunities for VLAN segmentation. The greater the number of hub connections, the greater the opportunities for VLAN segmentation down to individual users.

Each hub segment (as defined within individual hub architectures) connected to a switch port can be assigned to a VLAN. Stations that share a hub segment are all assigned to the same VLAN group. If an individual station needs to be reassigned to another VLAN, the station will be relocated to the appropriate corresponding hub module. The interconnected switch fabric handles the communication

between the switching ports and automatically determines the appropriate receiving segments. The more the shared hub can be broken into smaller groups, the greater the microsegmentation and the greater the VLAN flexibility for assigning individual users to VLAN groups.

This furthers the migration to a high-performance switching architecture within enterprise LANs. With this approach, network managers can configure their shared hubs as part of the VLAN architecture and can share traffic and network resources that directly attach to switching ports with VLAN designations.

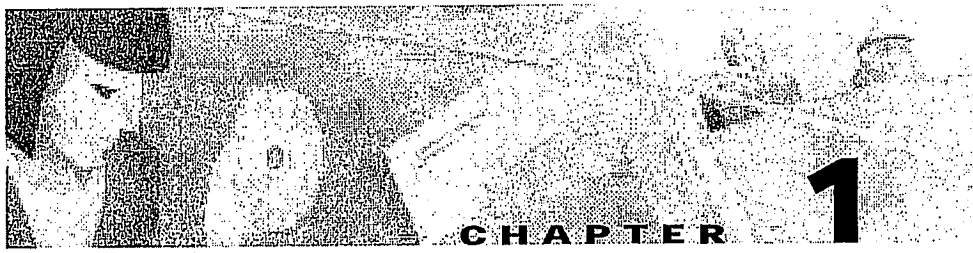
Centralized Administration Control

Control of network broadcasts; planning moves, adds and changes; and establishing access privileges to the network and secured resources are common functions of the central planning and administration group. VLAN communications facilitate this type of planning by providing effective VLAN management applications that can be centrally configured, managed, and monitored.

Conclusion

VLANs offer significant cost and performance benefits for a majority of the LANs installed today. These benefits are realized as network managers migrate to switched LAN architectures across the enterprise. And while VLANs are an integral part of ATM architectures, the concept and much of the technology has been designed into LAN-based switches that offer similar benefits across shared-LAN backbones. Further, end users' application need not change to realize these benefits. VLANs, as part of switching architecture, are invisible to end users. Finally, VLANs are more than simply a shared hub, routing, switching, or network management solution. It is the combination of all these components that provides powerful segmentation and efficient administration across the network.

Posted: Jul 14 15:32:01 1995



Product Overview

This chapter describes the Catalyst 5000 family switches. For detailed descriptions of system features and components, see Chapter 2, "Switch Description."

Note For a detailed description of supervisor engine operation in a redundant configuration, see Chapter 3, "Installing the Supervisor Engine," in the *Catalyst 5000 Family Supervisor Engine Installation Guide.*

The Catalyst 5000 family consists of five modular LAN switches:

- Catalyst 5002 Switch, page 1-5
- Catalyst 5000 Switch, page 1-7
- Catalyst 5505 Switch, page 1-7
- Catalyst 5509 Switch, page 1-8
- Catalyst 5500 Switch, page 1-10

Note Throughout this guide and all Catalyst 5000 family documents, "Catalyst 5000 family switches" refers to all of the Catalyst 5000 switches unless otherwise noted.

All switches share the same set of modules and software features—providing scalability while maintaining interoperability across all platforms.

All switches accept Ethernet, Fast Ethernet, Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Copper Distributed Data Interface (CDDI), and ATM modules. All switches, except the Catalyst 5002 switch, accept the Route Switch Module (RSM) and the RSM/Versatile Interface Processor 2 (VIP2). The Catalyst 5500 switch accepts LightStream 1010 ATM modules.

The Catalyst 5505, Catalyst 5509, and Catalyst 5500 switches accept redundant supervisor engines.

All switches can use Category 5 unshielded twisted-pair (UTP) cabling, coaxial cable, and multimode and single-mode fiber-optic cable.

Typically, Catalyst 5000 family Ethernet interfaces connect workstations and repeaters while the Fast Ethernet interfaces connect workstations, servers, switches, and routers. The nine-port Gigabit Ethernet switching module provides a high-performance gigabit switching backbone while the Supervisor Engine III Gigabit Ethernet interfaces serve as uplinks that aggregate traffic from high-density 10/100-Mbps wiring closets. The Gigabit EtherChannel switching module is used primarily for backbone interconnection of other high-performance Catalyst 5000 family switches and Cisco routers through Gigabit EtherChannel.

Table 1-1 lists and describes the Catalyst 5000 family switches.

Table 1-1 Catalyst 5000 Family Switches

Switch	Description	Features
Catalyst 5002	2-slot switch	• Catalyst 5002 switch with 155W power supply (see Figure 1-1) supports Supervisor Engines I, II, II G, and III G. Catalyst 5002 switch with 175W power supply with power factor correction (PFC) (see Figure 1-2) supports Supervisor Engines I, II, III, II G, and III G. The Catalyst 5002 switch also supports one additional switching module (Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI/CDDI, Token Ring, and ATM).

Table 1-1 Catalyst 5000 Family Switches (continued)

Switch	Description	Features
Catalyst 5002 (continued)		**Note** Your Catalyst 5002 switch has either a 155W power supply or 175W power supply with PFC. To determine which power supply your switch has, you can compare the front panel with Figure 1-1 and Figure 1-2. Alternatively, enter the **show system** command in Catalyst 5000 supervisor engine software release 3.1(2) or later. • Supports redundant AC-input or DC-input power supplies
Catalyst 5000	5-slot switch	• Supports Supervisor Engines I, II, II G, III, and III G and up to four additional switching modules (Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI/CDDI, Token Ring, and ATM) • Supports the RSM and RSM/VIP2 modules • Supports optional redundant AC-input or DC-input power supplies
Catalyst 5505	5-slot switch	• Supports Supervisor Engines II, II G, III, and III G and up to four additional switching modules (see the "Catalyst 5505 Switch" section on page 1-7 for a list of supported modules) • Supports the RSM and RSM/VIP2 modules • Supports redundant supervisor engines (two Supervisor Engine IIs, II Gs, IIIs, or III Gs); redundancy is supported only with like supervisor engines

Table 1-1 Catalyst 5000 Family Switches (continued)

Switch	Description	Features
Catalyst 5505 (continued)		• Supports Supervisor Engines II and II G but Supervisor Engine III or III G is recommended for utilizing all three buses effectively • Supports optional redundant AC-input or DC-input power supplies
Catalyst 5509	9-slot switch	• Supports Supervisor Engines II, II G, III, or III G and up to eight additional switching modules (see the "Catalyst 5509 Switch" section on page 1-8 for a list of supported modules) • Supports the RSM and RSM/VIP2 modules • Supports redundant supervisor engines (two Supervisor Engine IIs, II Gs, IIIs, or III Gs); redundancy is supported only with like supervisor engines • Supports Supervisor Engines II and II G but Supervisor Engine III or III G is recommended for utilizing all three buses effectively • Supports optional redundant AC-input or DC-input power supplies
Catalyst 5500	13-slot switch	• Supports Supervisor Engines II, II G, III, or III G and up to 11 additional switching modules (see the "Catalyst 5500 Switch" section on page 1-10 for a list of supported modules) • Supports the RSM and RSM/VIP2 modules • Supports redundant supervisor engines (two Supervisor Engine IIs, II Gs, IIIs, or III Gs); redundancy is supported only with like supervisor engines

Table 1-1 Catalyst 5000 Family Switches (continued)

Switch	Description	Features
Catalyst 5500 (continued)		• Supports Supervisor Engine II and II G but Supervisor Engine III or III G is recommended for utilizing all three buses effectively • Supports optional redundant AC-input or DC-input power supplies

Catalyst 5002 Switch

The Catalyst 5002 switch chassis has two slots. Slot 1 is for the supervisor engine, which provides switching, local and remote management, and multiple uplink interfaces. Slot 2 is available for switching modules.

The Catalyst 5002 switch comes equipped either with a 155W power supply or a 175W power supply with PFC. Figure 1-1 shows the Catalyst 5002 switch with a 155W power supply. Figure 1-2 shows the Catalyst 5002 switch with a 175W power supply with PFC.

Note The Catalyst 5002 switch with 155W power supply does not support Supervisor Engine III.

The Catalyst 5002 switch has a 1.2-Gbps media-independent switching fabric that provides the connections between power supplies, the supervisor engine, and the switching module. This switching fabric supports wire-speed switching for the supported line modules. See Table 1-1 for additional information.

Figure 1-1 Catalyst 5002 Switch with 155W Power Supply

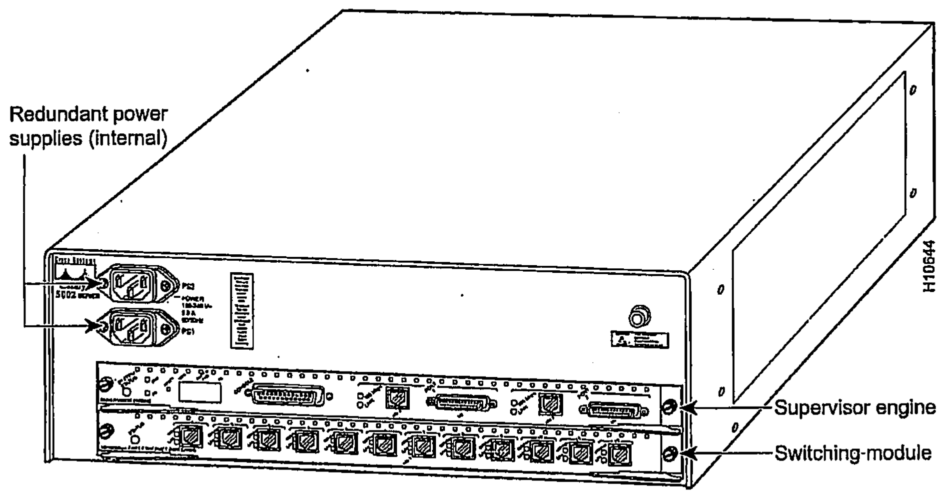
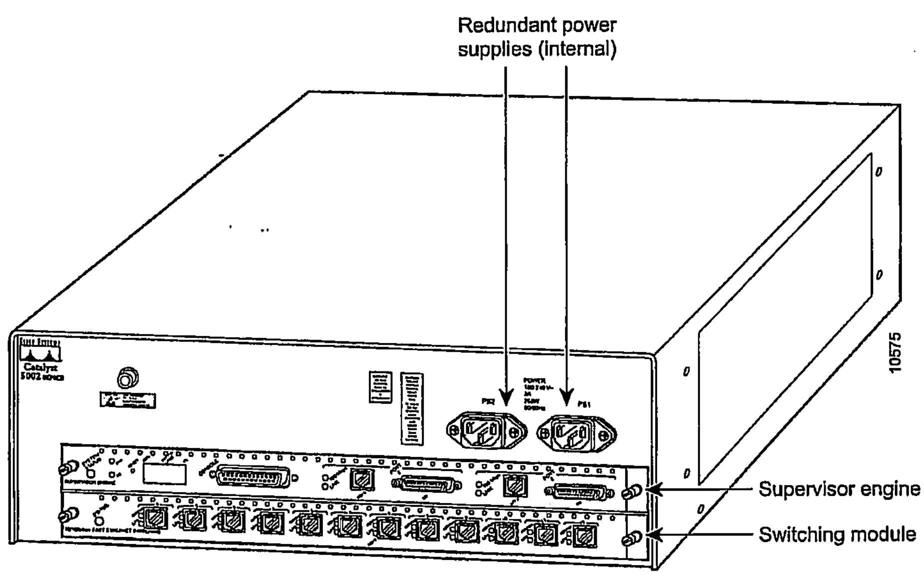


Figure 1-2 Catalyst 5002 Switch with 175W Power Supply with PFC

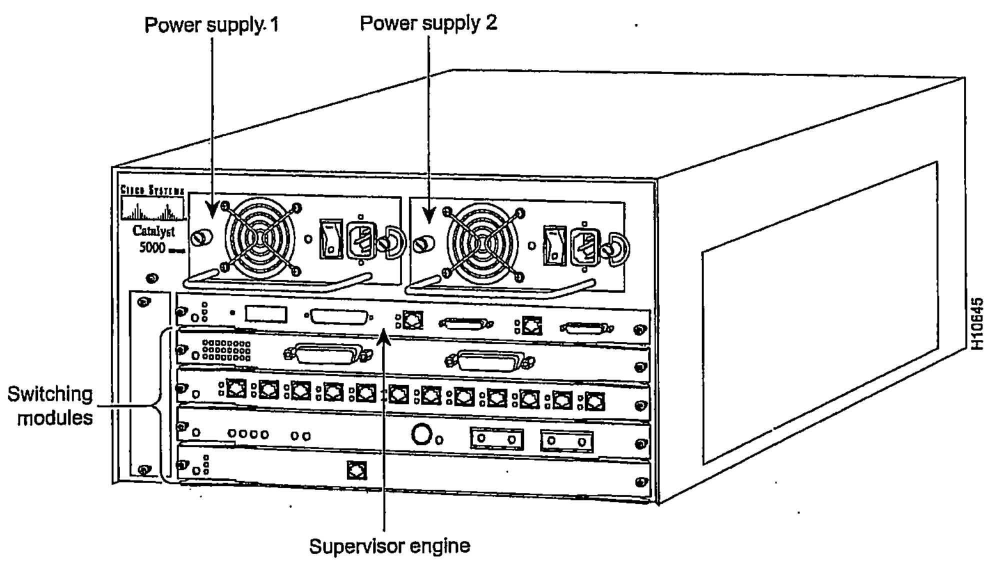


Catalyst 5000 Switch

The Catalyst 5000 switch chassis has five slots. (See Figure 1-3.) Slot 1 is for the supervisor engine, which provides switching, local and remote management, and dual uplink interfaces. Slots 2 through 5 are available for switching modules.

The Catalyst 5000 switch has a 1.2-Gbps media-independent switching fabric that provides the connections between power supplies, the supervisor engine, and the switching modules. This switching fabric supports wire-speed switching for the supported line modules. See Table 1-1 for additional information.

Figure 1-3 Catalyst 5000 Switch



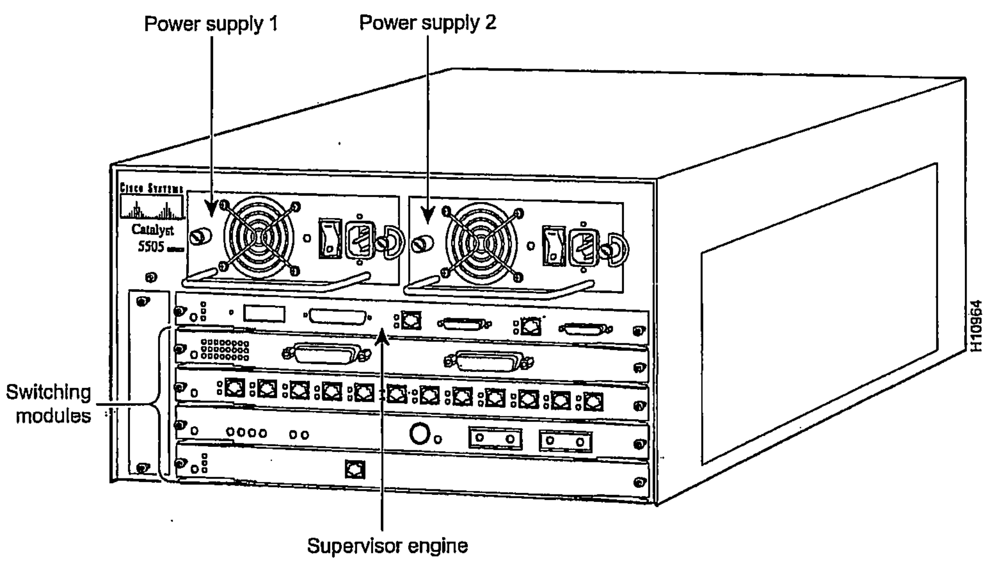
Catalyst 5505 Switch

The Catalyst 5505 switch chassis has five slots. (See Figure 1-4.) Slot 1 is for the supervisor engine, which provides switching, local and remote management, and dual uplink interfaces. Slot 2 can contain an additional redundant supervisor

engine, which acts as a backup function in case the first module fails. A failure of the active supervisor engine is detected by the standby module, which then takes control of the supervisor engine switching functions. If a redundant supervisor engine is not required, slots 2 through 5 are available for switching modules.

The Catalyst 5505 switch is an enhanced version of the Catalyst 5000 switch with a three-bus, 3.6-Gbps media-independent switching fabric that provides the connections between power supplies, the supervisor engine, and the switching modules. The 3.6-Gbps media-independent fabric supports Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI/CDDI, ATM LAN Emulation (LANE), ATM dual physical layer (PHY) DS3, RSM, and RSM/VIP2 modules. See Table 1-1 for additional information.

Figure 1-4 Catalyst 5505 Switch



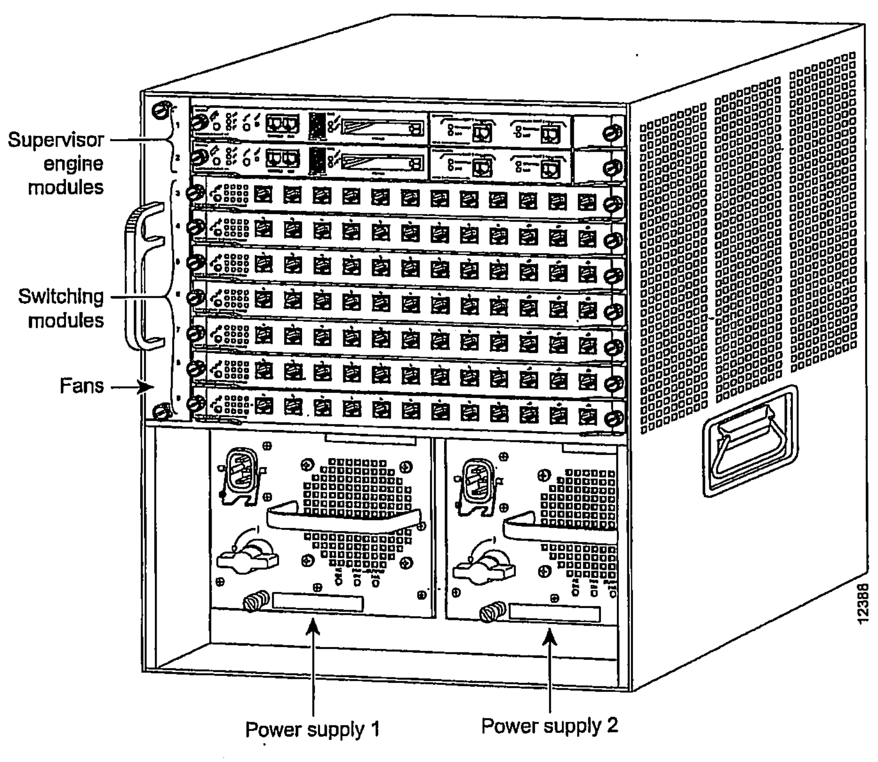
Catalyst 5509 Switch

The Catalyst 5509 switch chassis has nine slots. (See Figure 1-5.) Slot 1 is for the supervisor engine, which provides switching, local and remote management, and multiple uplink interfaces. Slot 2 can contain an additional redundant supervisor

engine, which acts as a backup in case the first module fails. A failure of the active supervisor engine is detected by the standby module, which then takes control of the supervisor engine switching functions. If a redundant supervisor engine is not required, slots 2 through 9 are available for switching modules.

The Catalyst 5509 switch has a three-bus, 3.6-Gbps media-independent switching fabric that provides the connections between power supplies, the supervisor engine, and the switching modules. The three-bus, 3.6-Gbps backplane is accessible from all nine slots. The 3.6-Gbps media-independent fabric supports Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI/CDDI, ATM LANE, ATM dual PHY DS3, RSM, and RSM/VIP2 modules. See Table 1-1 for additional information.

Figure 1-5 Catalyst 5509 Switch



Catalyst 5500 Switch

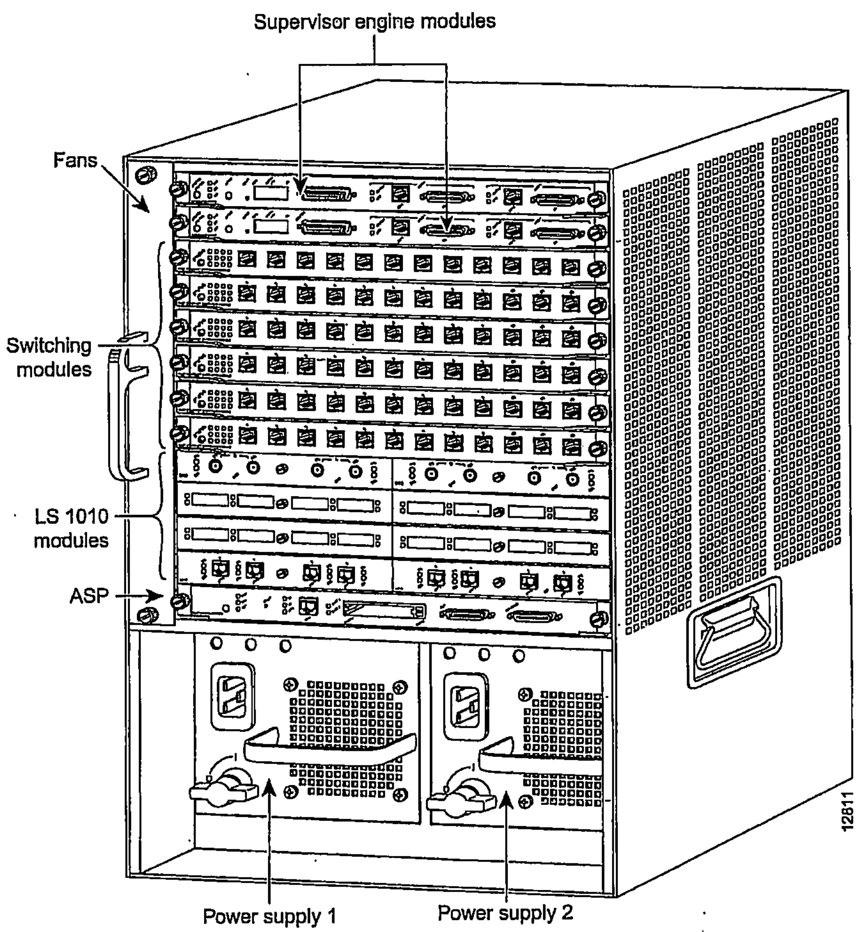
The Catalyst 5500 switch chassis has 13 slots. (See Figure 1-6.) Slot 1 is for the supervisor engine, which provides switching, local and remote management, and multiple uplink interfaces. Slot 2 can contain an additional redundant supervisor engine, which acts as a backup in case the first module fails. A failure of the active supervisor engine is detected by the standby module, which takes control of supervisor engine switching functions. If a redundant supervisor engine is not required, slot 2 is available for any switching module.

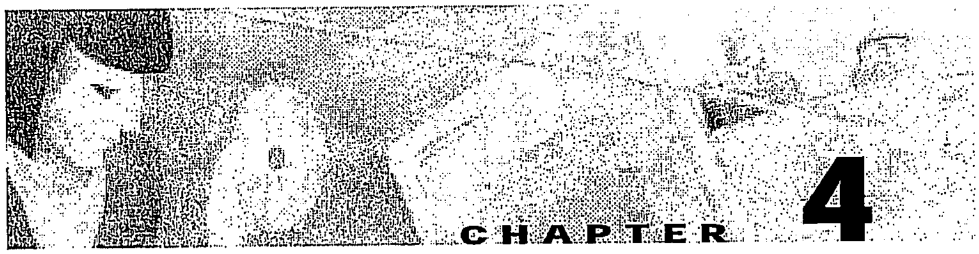
Slots 3 through 12 are available for any combination of switching modules.

Slot 13 is a dedicated slot, which accepts only the ATM switch processor (ASP) module or the Catalyst 8510 Campus Switch Router (CSR) switch route processor (SRP). When using the ASP in slot 13, the Catalyst 5500 switch accepts LightStream 1010 ATM port adapters in slots 9 through 12. When using the Catalyst 8510 CSR SRP in slot 13, the Catalyst 5500 switch accepts Catalyst 8510 CSR modules in slots 9 through 12.

The Catalyst 5500 switch has a 3.6-Gbps media-independent switch fabric and a 5-Gbps cell-switch fabric. The backplane provides the connection between power supplies, supervisor engine, switching modules, and backbone module. The 3.6-Gbps media-independent fabric supports Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI/CDDI, ATM LANE, ATM dual PHY DS3, RSM, and RSM/VIP2 modules. The 5-Gbps cell-based fabric supports an ASP module and ATM port adapters. See Table 1-1 for additional information.

Figure 1-6 Catalyst 5500 Switch





Installing the Switch

Warning **Before you install, operate, or service the system, read the *Site Preparation and Safety Guide*. This guide contains important safety information you should know before working with the system.**

Note The information in this chapter applies to all Catalyst 5000 family switches unless otherwise noted.

This chapter describes how to install the Catalyst 5000 family switch in a rack. For first-time installations, perform the procedures in the following sections in the order listed:

- Checking the Contents, page 4-2
- Rack-Mounting the Switch, page 4-2

For information on installing the supervisor engines and verifying switch operation, see Chapter 3, "Installing the Supervisor Engine," in the *Catalyst 5000 Family Supervisor Engine Installation Guide*.

Note Before starting the installation procedures in this chapter, use the site planning checklist in Chapter 3, "Site Planning," to verify that all site planning activities were completed.

Checking the Contents

Note Do not discard the shipping container when you unpack the switch. Flatten the shipping cartons and store them with the pallet (supplied with the Catalyst 5509 and Catalyst 5500 switches). You will need these containers if you need to move or ship the switch in the future. Repacking instructions are provided in Appendix B, "Repacking a Switch."

To check the contents of the shipping container, follow these steps:

Step 1 Check the contents of the accessories box against the Accessories Box Components Checklist and the packing slip. Verify that you received all listed equipment, which should include the following:

- Switch hardware and software documentation, if ordered
- Optional equipment that you ordered, such as network interface cables, transceivers, or special connectors

Step 2 Check the switching modules in each slot. Ensure that the configuration matches the packing list and that all the specified interfaces are included.

Step 3 To begin installation, proceed to the "Rack-Mounting the Switch" section on page 4-2.

Rack-Mounting the Switch

A standard rack-mount kit is included for mounting the switch in a standard 19-inch (48.3 cm) equipment rack with two unobstructed outer posts, with a minimum depth (between the front and rear mounting posts) of 19.25 inches (48.9 cm) and a maximum depth of 32 inches (81.3 cm). This kit is not suitable for use with racks with obstructions (such as a power strip) that could impair access to switch field-replaceable units (FRUs).

Caution Before installing the chassis in a rack, read the "Checking the Contents" section on page 4-2 to familiarize yourself with the proper site and environmental conditions. Failure to read and follow these guidelines could lead to an unsuccessful installation and possible damage to the system and components.

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Rack-Mounting Guidelines

Before rack-mounting the switch, ensure the following:

- The equipment rack is the proper size.
  - The width of the rack, between the two front mounting strips or rails, must be 17.75 inches (45.09 cm).
  - The depth of the rack, between the front and rear mounting strips, must be at least 19.25 inches (48.9 cm) but not more than 32 inches (81.3 cm).
  - The rack must have sufficient vertical clearance to insert the chassis. The chassis heights are as follows:

    Catalyst 5002 switch—5.75 inches (14.6 cm)

    Catalyst 5000 and Catalyst 5505 switches—10.4 inches (26.4 cm)

    Catalyst 5509 switch—20 inches (50.8 cm)

    Catalyst 5500 switch—25 inches (63.5 cm)
- The equipment rack is stable and in no danger of falling over.
  - Ensure that the shelf is constructed to support the weight and dimensions of the chassis. For physical specifications, see Appendix A, "Specifications."
  - We recommend that you bolt the rack to the floor.

- Mount the unit at the bottom of the rack if it is the only unit in the rack.
- Install heavier equipment in the lower half of the rack to maintain a low center of gravity and prevent the rack from becoming top-heavy and tipping over.
- Install the stabilizers before mounting or servicing the switch in the rack (if the rack is provided with stabilizing devices).

• The equipment rack is properly ventilated.

- Install the chassis in an enclosed rack only if it has adequate ventilation or an exhaust fan; use an open rack whenever possible.
- Ensure that the ambient temperature of the rack environment does not exceed a maximum temperature of 104°F (40°C). Note that if the switch is installed in a closed-or multiunit rack assembly, the ambient operating temperature of the rack environment might be higher than the ambient room temperature.
- Note that a ventilation system in a closed rack that is too powerful might also prevent cooling by creating negative pressure around the chassis and redirecting the air away from the chassis intake vent. If necessary, operate the chassis with the rack open.
- To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.
- Use baffles correctly to assist in cooling the chassis.
- Note that equipment near the bottom of a rack may generate excessive heat that is drawn upward and into the intake ports of equipment above, leading to overtemperature conditions in the chassis at or near the top of the rack.
- Consider the equipment and cabling that is already installed in the rack. Ensure that cables from other equipment will not obstruct the airflow through the chassis or impair access to the power supplies or switching modules. Route cables away from field-replaceable-units to avoid disconnecting cables unnecessarily for equipment maintenance or upgrades.
- Allow at least 3 to 4 feet (91.4 to 121.9 cm) of clearance behind the rack for maintenance and removal of switch assemblies. If the rack is mobile, you can push it back within 1 foot (30.45 cm) of a wall or cabinet for normal operation and pull it out when necessary for maintenance.

Lifting the Chassis Safely

Two people are required to lift a Catalyst 5000, Catalyst 5505, Catalyst 5509, or Catalyst 5500 chassis. Whenever you lift the chassis or any heavy object, follow these guidelines:

- Never attempt to lift a chassis by yourself. The size and weight of a chassis requires two people to safely lift and move it without causing injury or damaging the equipment.
- Ensure that your footing is solid, and balance the weight of the chassis between your feet.
- Lift the chassis slowly; never move suddenly or twist your body as you lift.
- Keep your back straight and lift with your legs, not your back. If you must bend down to lift the chassis, bend at the knees, not at the waist, to reduce the strain on your lower back muscles.
- Leave all switch FRUs installed (such as switching modules, power supplies, and fan assembly).
- Always disconnect all external cables before lifting or moving the chassis.

The chassis is not intended to be moved frequently. Before you install the switch, ensure that your site is properly prepared so that you can avoid moving the chassis later to accommodate power sources and network connections.

Required Installation Tools

The following tools and equipment are required to install the chassis:

- Number 1 and number 2 Phillips screwdrivers to tighten the captive installation screws on most systems
- 3/16-inch flat-blade screwdriver for the captive installation screws on the supervisor engine and switch modules in some systems
- Antistatic mat or antistatic foam in case you need to remove switch modules to troubleshoot the installation
- Your own ESD grounding strap or the disposable ESD strap included with the system

The following tools and equipment are required to install the chassis in a rack:

- Rack-mount kit
- Cable management kit
- Tape measure and level

Rack-Mounting Procedures

Proceed to the rack-mount installation procedure for the type of switch you are installing:

- Rack-Mounting the Catalyst 5002 Switch, page 4-6
- Rack-Mounting the Catalyst 5000 and Catalyst 5505 Switches, page 4-9
- Rack-Mounting the Catalyst 5509 Switch, page 4-13
- Rack-Mounting the Catalyst 5500 Switch, page 4-19

Rack-Mounting the Catalyst 5002 Switch

Use this procedure to install the Catalyst 5002 switch in a rack:

Note The procedures are the same for both the AC-input and DC-input power supply models. The figures shown in this section reflect the AC-input power supply model.

Step 1 Prepare for installation as follows:

a. Place the chassis on the floor or on a sturdy table as close as possible to the rack. Leave enough clearance to allow you to move around the chassis.

b. Use a tape measure to measure the depth of the rack. Measure from the outside of the front mounting posts to the outside of the rear mounting strip. The depth must be at least 19.25 inches (48.9 cm) but not greater than 32 inches (81.3 cm).

c. Measure the space between the inner edges of the left front and right front mounting posts to ensure that it is 17.75 inches (45.09 cm) wide. (The chassis is 17.25 inches [43.8 cm] wide and must fit between the mounting posts.)

d: Open the rack-mount kit and see the component checklist in Table 4-1 to verify that all parts are included.

Table 4-1 Catalyst 5002 Switch: Rack-Mount Kit Checklist

Quantity	Part Description	Received
2	L brackets	
4	M4 Phillips pan-head screws	
6	12-24 x 3/4-inch Phillips binder-head screws	

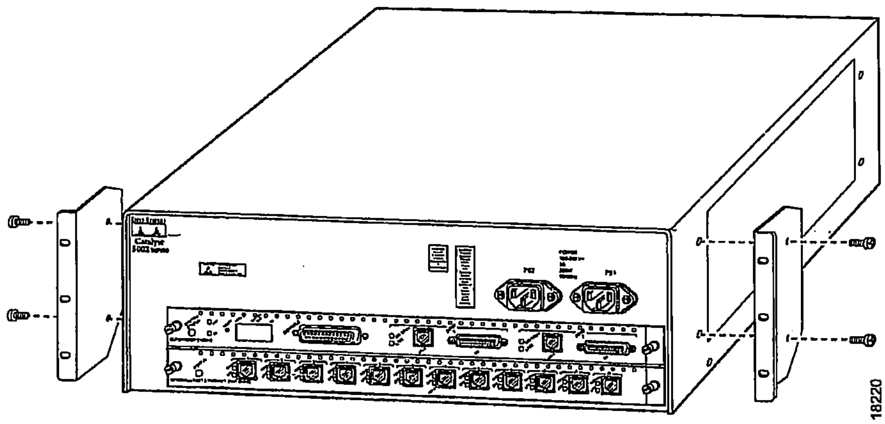
Note Figure 4-1 illustrates how to attach the front of the switch to the rack. You can also attach the rear of the switch to the rack, depending on the configuration of your rack.

Step 2 Note that the L brackets connect the chassis to the rack. You can mount the L brackets to the front or rear mounting holes of the chassis, depending on which end is in the front of the rack.

Note Some equipment racks provide a power strip along the length of one of the rear posts. If your rack has this feature, consider the position of the strip when planning fastener points. Before you install the L brackets on the chassis, determine whether you will install the chassis from the front or the rear of the rack.

Attach the left and right L brackets using the four M4 Phillips pan-head screws provided in the rack-mount kit. (See Figure 4-1.)

Figure 4-1 Catalyst 5002 Switch: Attaching the L Brackets



Step 3 Install the chassis in the rack as follows:

a. Position the chassis in the rack as follows (see Figure 4-2):
   - If the chassis front panel is in the front of the rack, insert the rear of the chassis between the mounting posts.
   - If the rear of the chassis is in the front of the rack, insert the front of the chassis between the mounting posts.

b. Align the mounting holes in the L bracket with the mounting holes in the equipment rack.

c. Secure the chassis using six (three per side) 12-24 x-3/4-inch screws through the elongated holes in the L bracket and into the threaded holes in the mounting post.

d. Use a tape measure and level to ensure that the chassis is installed straight and level.

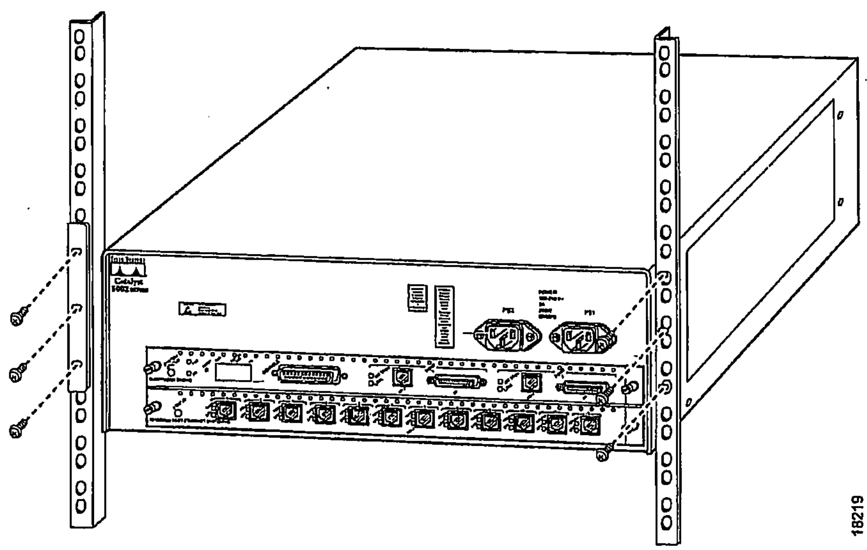
Step 4 From the rear of the chassis, do the following:

a. Check the ejector levers to ensure that the supervisor engine and the switching module are installed securely.

b. Tighten any loose captive installation screws on the supervisor engine and switching module.

Step 5 Note that the Catalyst 5002 switch powers up when you connect the power supply cords (do not power up the supplies at this point).

Figure 4-2 Catalyst 5002 Switch: Installing the Switch in the Rack



Rack-Mounting the Catalyst 5000 and Catalyst 5505 Switches

Use this procedure to install the Catalyst 5000 switch or Catalyst 5505 switch in a rack:

Step 1 Prepare for installation as follows:

a. Place the chassis on the floor or on a sturdy table as close as possible to the rack. Leave enough clearance to allow you to move around the chassis.

b. Use a tape measure to measure the depth of the rack. Measure from the outside of the front mounting posts to the outside of the rear mounting strip. The depth must be at least 19.25 inches (48.9 cm) but not greater than 32 inches (81.3 cm).

c. Measure the space between the inner edges of the left-front and right front mounting posts to ensure that it is 17.75 inches (45.09 cm) wide. (The chassis is 17.25 inches [43.8 cm] wide and must fit between the mounting posts.)

d. Open the rack-mount kit and use the checklist in Table 4-2 to verify that all parts are included.

Table 4-2 Catalyst 5000 and Catalyst 5505 Switches: Rack-Mount Kit Checklist

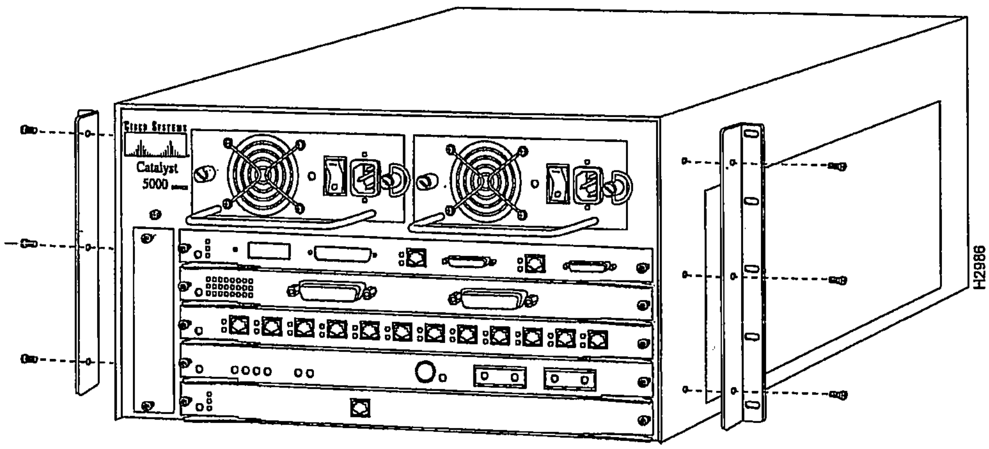
Quantity	Part Description	Received
2	L brackets (left and right)	
6	M4 Phillips countersunk-head screws	
8	12-24 x 3/4-inch Phillips binder-head screws	
8	10-32 x 3/4-inch slotted binder-head screws	

Step 2 Note that the L brackets connect the chassis to the rack. Install the L brackets as follows:

a. Remove the six screws from either the front or rear of the switch side cover panels, depending on which end of the chassis will be at the front of the rack.

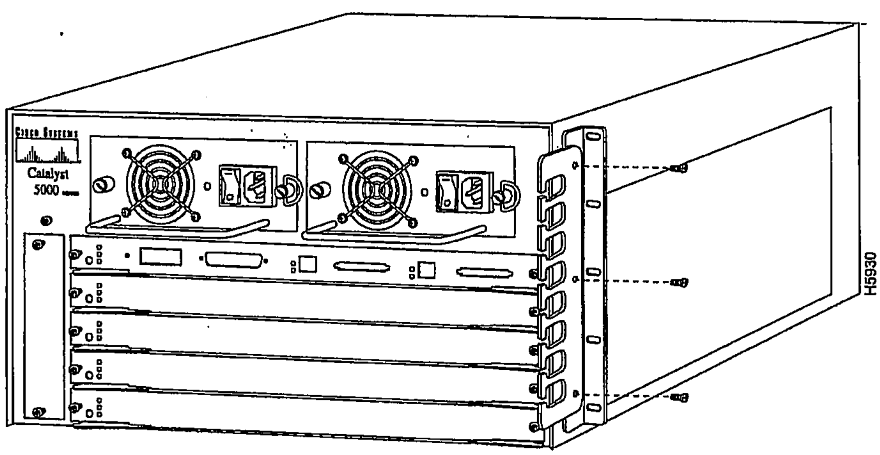
b. Attach the L brackets to the left and right sides of the chassis using the six M4 Phillips countersunk-head screws provided in the rack-mount kit. (See Figure 4-3.)

Figure 4-3 Catalyst 5000 and Catalyst 5505 Switches: Attaching the L Brackets



c. Attach the cable guide, if needed, using the M3 screws provided in the cable management kit. The cable guide attaches to the L bracket. Attach the cable guide to the right side of the switch to prevent the cables from obscuring module LEDs. (See Figure 4-4.)

Figure 4-4 Catalyst 5000 and Catalyst 5505 Switches: Attaching the Cable Guide



Step 3 Install the chassis in the rack as follows:

Note You should have a third person on hand to assist in this step.

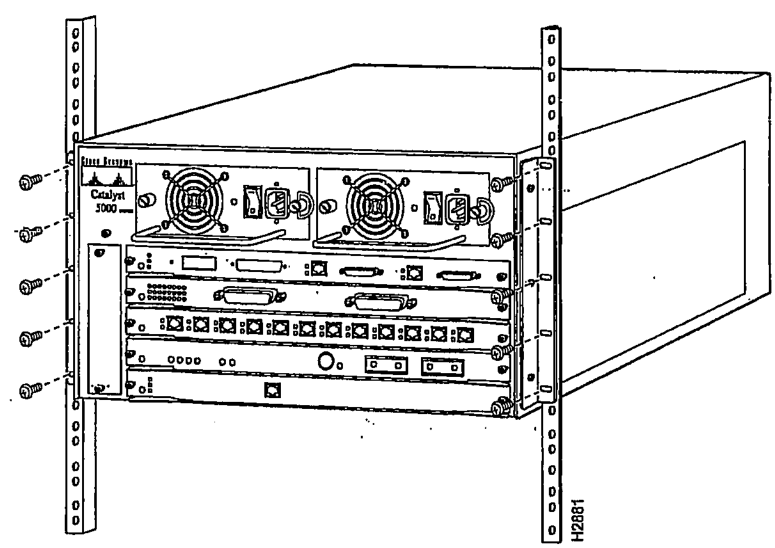
a. With a person standing at each side of the chassis, grasp the bottom edge of the chassis with one hand near the front and the other near the back. Slowly lift the chassis in unison. Avoid sudden twists or moves to prevent injury.

b. Position the chassis in the rack as follows (see Figure 4-5):

- If the front of the chassis (front panel) is at the front of the rack, insert the rear of the chassis between the mounting posts.
- If the rear of the chassis is at the front of the rack, insert the front of the chassis between the mounting posts.

c. Align the five L bracket mounting holes with the five front mounting post mounting holes.

Figure 4-5 Catalyst 5000 and Catalyst 5505 Switches: Installing the Switch in the Rack



d. *A third person* should install the 10-32 x 3/4-inch slotted binder-head mounting screws through the elongated holes in the L bracket and into the threaded holes in the mounting post.

e. Use a tape measure and level to ensure that the chassis is installed straight and level.

Step 4 From the rear of the chassis, do the following:

a. Check the ejector levers to ensure that the supervisor engine and all switching modules are securely installed.

b. Tighten any loose captive installation screws on the supervisor engine and switching modules.

Step 5 Connect the power supplies to the site power following the procedures in the "Removing and Replacing the Power Supply" section on page 5-2. (Do not turn on the power supplies at this point.)

Rack-Mounting the Catalyst 5509 Switch

Use this procedure to install the Catalyst 5509 switch in a rack:

Step 1 Prepare for installation as follows:

a. Place the chassis on the floor or on a sturdy table as close as possible to the rack. Leave enough clearance to allow you to move around the chassis.

b. Install the power supplies in the chassis by following the procedures in the "Removing and Replacing the Power Supply" section on page 5-2. (Do not connect the power cords at this point.)

c. Use a tape measure to measure the depth of the rack. Measure from the outside of the front mounting posts to the outside of the rear mounting strip. The depth must be at least 19.25 inches (48.9 cm) but not greater than 32 inches (81.3 cm).

d. Measure the space between the inner edges of the left front and right front mounting posts to ensure that it is 17.75 inches (45.09 cm) wide. (The chassis is 17.25 inches [43.8 cm] wide and must fit between the mounting posts.)

e. Open the rack-mount kit and use the checklist in Table 4-3 to verify that all parts are included.

Table 4-3 Catalyst 5509 Switch: Rack-Mount Kit Checklist

Quantity	Part Description	Received
2	L brackets	
8	M4 Phillips countersunk-head screws	
8	12-24 x 3/4-inch Phillips binder-head screws	
8	10-32 x 3/4-inch Phillips binder-head screws	
2	Shelf brackets	
1	Crossbar bracket	
2	M3 Phillips pan-head screws	

Step 2 Note that the two shelf brackets support the weight of the chassis in the rack. Install the shelf brackets as follows:

Caution If the rack is on wheels, ensure that the brakes are engaged or that the rack is otherwise stabilized.

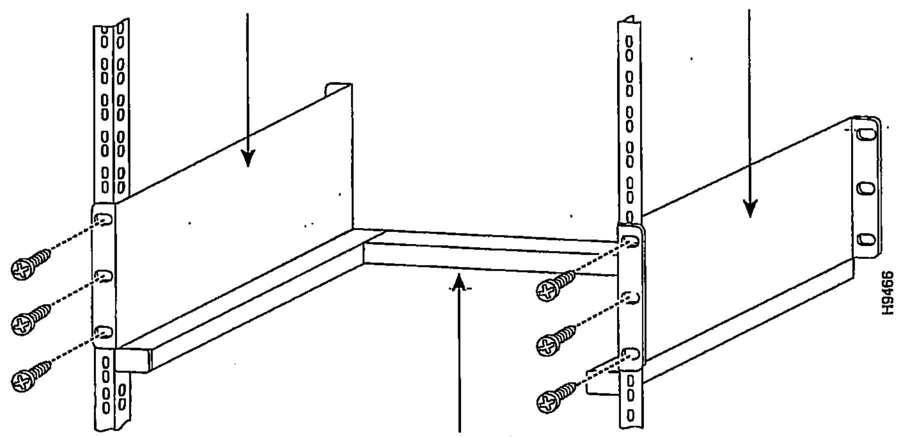
a. Position the shelf brackets in the rack. (See Figure 4-6.)

b. Secure the shelf brackets by using six (three per side) 12-24 x 3/4-inch or 10-32 x 3/4-inch screws.

c. Attach the crossbar bracket to the back of the shelf brackets using two M3 screws.

Note No shelf is required with this assembly; the shelf brackets support the chassis in the rack.

Figure 4-6 Catalyst 5509 Switch: Installing the Shelf Brackets

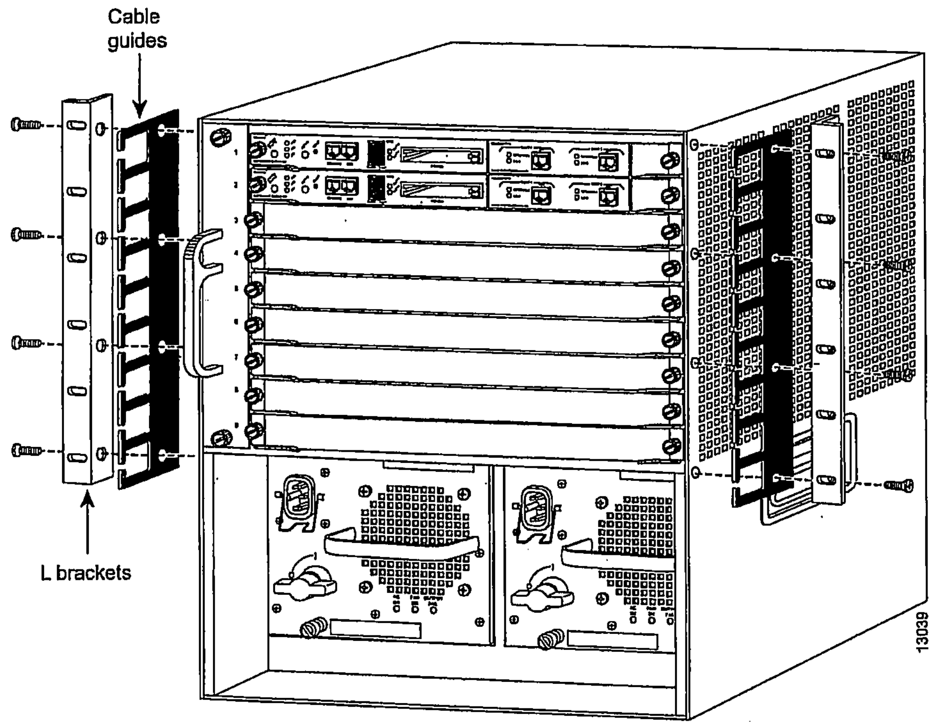


Step 3 Note that the L brackets connect the chassis to the rack. Install the L brackets by attaching the left and right L brackets using the eight M4 Phillips countersunk-head screws provided in the rack-mount kit. (See Figure 4-7.)

Note Some equipment racks provide a power strip along the length of one of the rear posts. If your rack has this feature, consider the position of the strip when planning fastener points. Before you install the L brackets on the chassis, determine whether you will install the chassis from the front or the rear of the rack.

Note If you are installing cable guides, place the cable guides inside the L brackets, between the L bracket and the chassis. Secure the cable guides to the chassis using the same screws (and chassis holes) as the L brackets. (See Figure 4-7.) The cable guides and screws are provided in the cable management kit.

Figure 4-7 Catalyst 5509 Switch: Attaching L Brackets and Cable Guides



Step 4 Install the chassis in the rack as follows:

> **Note** You should have a third person available to assist in this step.

a. With a person standing at each side of the chassis, grasp the bottom edge of the chassis with one hand near the front and the other near the back. Slowly lift the chassis in unison. Avoid sudden twists or moves to prevent injury.

b. Position the chassis in the rack as follows (see Figure 4-8):

- If the front of the chassis (front panel) is at the front of the rack, insert the rear of the chassis between the mounting posts.

- If the rear of the chassis is at the front of the rack, insert the front of the chassis between the mounting posts.

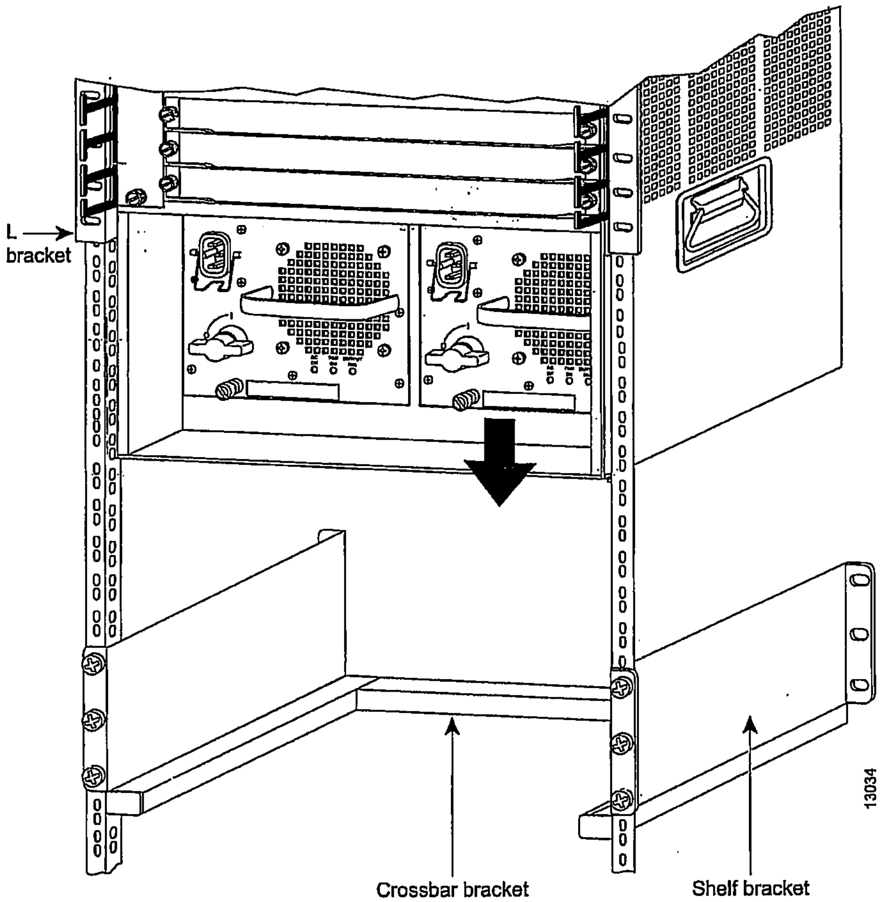
c. Place the chassis on the shelf brackets.

d. Align the mounting holes in the L bracket with the mounting holes in the equipment rack.

e. A third person should install the eight (four per side) 12-24 x 3/4-inch or 10-32 x 3/4-inch screws through the elongated holes in the L bracket and into the threaded holes in the mounting post.

f. Use a tape measure and level to ensure that the chassis is installed straight and level.

Figure 4-8 Catalyst 5509 Switch: Installing the Switch in the Rack



Step 5 Check the ejector levers to ensure that the supervisor engine and all switching modules are installed securely.

Step 6 Tighten any loose captive installation screws on the supervisor engine and switching modules.

Step 7 Connect the power supplies to the site power by following the procedures in the "Removing and Replacing the Power Supply" section on page 5-2. (Do not turn on the power supplies at this point.)

Rack-Mounting the Catalyst 5500 Switch

Use this procedure to install the Catalyst 5500 switch in a rack:

Step 1 Prepare for installation as follows:

a. Place the chassis on the floor or on a sturdy table as close as possible to the rack. Leave enough clearance to allow you to move around the chassis.

b. Install the power supplies in the chassis by following the procedures in "Removing and Replacing the Power Supply" section on page 5-2. (Do not connect the power cords at this point.)

c. Use a tape-measure to measure the depth of the rack. Measure from the outside of the front mounting posts to the outside of the rear mounting strip. The depth must be at least 19.25 inches (48.9 cm) but not greater than 32 inches (81.3 cm).

d. Measure the space between the inner edges of the left front and right front mounting posts to ensure that it is 17.75 inches (45.09 cm) wide. (The chassis is 17.25 inches [43.8 cm] wide and must fit between the mounting posts.)

e. Open the rack-mount kit and use the checklist in Table 4-4 to verify that all parts are included.

Table 4-4 Catalyst 5500 Switch: Rack-Mount Kit Checklist

Quantity	Part Description	Received
2	L brackets	
10	M4 Phillips countersunk-head screws	
10	12-24 x 3/4-inch Phillips binder-head screws	
10	10-32 x 3/4-inch Phillips binder-head screws	
2	Shelf brackets	

Table 4-4 Catalyst 5500 Switch Rack-Mount Kit Checklist (continued)

Quantity	Part Description	Received
1	Crossbar bracket	
2	M3 Phillips pan-head screws	

Step 2 Note that the two shelf brackets support the weight of the chassis in the rack. Install the shelf brackets as follows:

Caution If the rack is on wheels, ensure that the brakes are engaged or that the rack is otherwise stabilized.

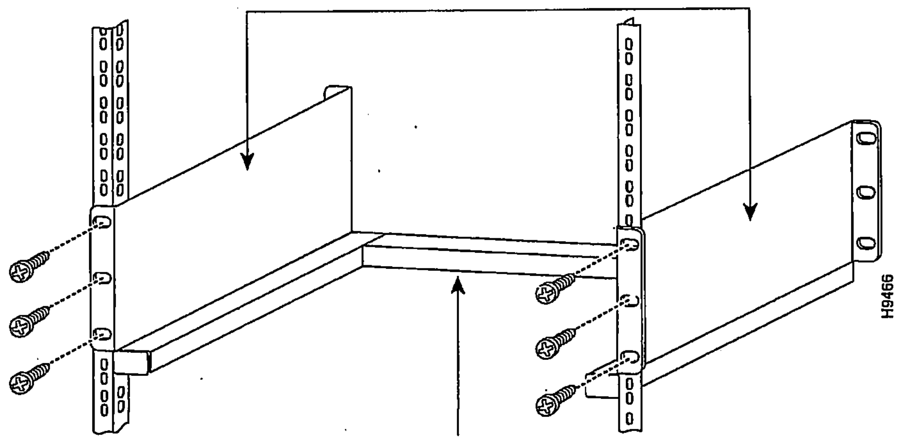
a. Position the shelf brackets in the rack (see Figure 4-9).

b. Secure the shelf brackets by using six (three per side) 12-24 x 3/4-inch or 10-32 x 3/4-inch screws.

c. Attach the crossbar bracket to the back of the shelf brackets using two M3 screws.

Note No shelf is required with this assembly; the shelf brackets support the chassis in the rack.

Figure 4-9 Catalyst 5500: Installing the Shelf Brackets

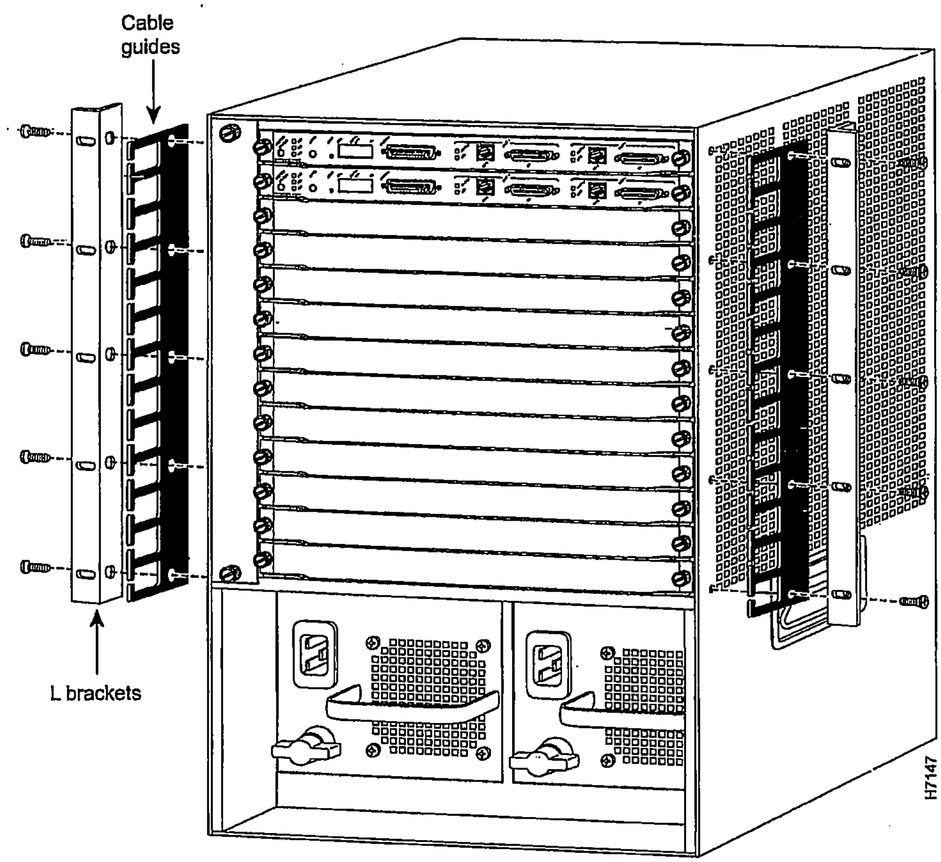


Step 3 Note that the L brackets connect the chassis to the rack. Install the L brackets by attaching the left and right L brackets using the ten M4 Phillips countersunk-head screws provided in the rack-mount kit. (See Figure 4-10.)

Note Some equipment racks provide a power strip along the length of one of the rear posts. If your rack has this feature, consider the position of the strip when planning fastener points. Before you install the L brackets on the chassis, determine whether you will install the chassis from the front or the rear of the rack.

Note If you are installing cable guides, place the cable guides inside the L brackets, between the L bracket and the chassis. Secure the cable guides to the chassis using the same screws (and chassis holes) as the L brackets. (See Figure 4-10.) The cable guides and screws are provided in the cable management kit.

Figure 4-10 Catalyst 5500 Switch: Attaching L Brackets and Cable Guides



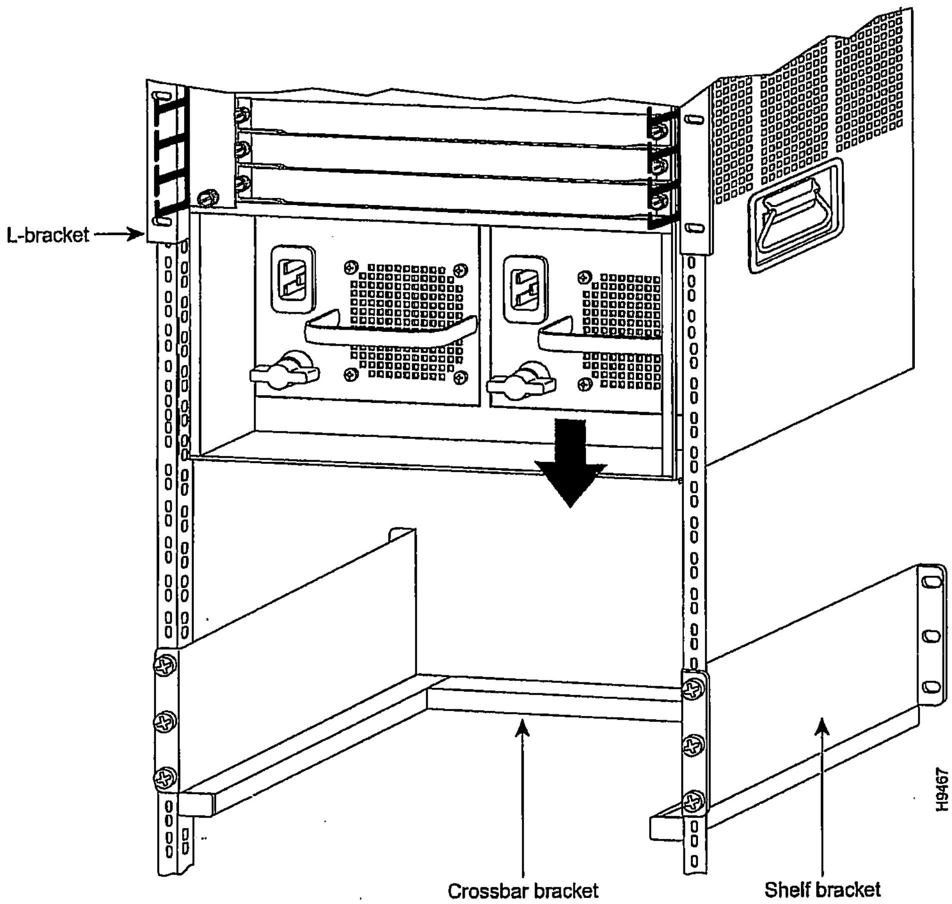
Step 4 Install the chassis in the rack as follows:

> **Note** You should have a third person available to assist in this step.

a. With a person standing at each side of the chassis, grasp the bottom edge of the chassis with one hand near the front and the other near the back. Slowly lift the chassis in unison. Avoid sudden twists or moves to prevent injury.

b. Position the chassis in the rack as follows (see Figure 4-11):
   - If the front of the chassis (front panel) is at the front of the rack, insert the rear of the chassis between the mounting posts.
   - If the rear of the chassis is at the front of the rack, insert the front of the chassis between the mounting posts.
c. Place the chassis on the shelf brackets.
d. Align the mounting holes in the L bracket with the mounting holes in the equipment rack.
e. A third person should install the ten (five per side) 12-24 x 3/4-inch or 10-32 x 3/4-inch screws through the elongated holes in the L bracket and into the threaded holes in the mounting post.
f. Use a tape measure and level to ensure that the chassis is installed straight and level.

Figure 4-11 Catalyst 5500 Switch: Installing the Switch in the Rack



Step 5 Check the ejector levers to ensure that the supervisor engine and all switching modules are installed securely.

Step 6 Tighten any loose captive installation screws on the supervisor engine and switching modules.

Step 7 Connect the power supplies to the site power by following the procedures in the "Removing and Replacing the Power Supply" section on page 5-2. (Do not turn on the power supplies at this point.)

CHAPTER 1

Product Overview

The Catalyst 1200 series switch is an Ethernet-to-Ethernet and Ethernet-to-CDDI/FDDI switch that provides high-speed transparent bridging between Ethernets and high-speed translational bridging between Ethernet and Copper Distributed Data Interface (CDDI) or Fiber Distributed Data Interface (FDDI). The Catalyst 1200 series switch includes four models: WS-C1201, WS-C1202, WS-C1211, and WS-C1212. Using content-addressable memory (CAM) technology, models WS-C1201 and WS-C1211 can learn up to 1,024 Ethernet addresses, and models WS-C1202 and WS-C1212 can learn up to 4,096 Ethernet addresses.

The switch has eight 10-Mbps Ethernet ports and two 100-Mbps CDDI or FDDI ports that comply fully with the FDDI and American National Standards Institute (ANSI) draft specifications for CDDI multilevel transmission (MLT-3) A and B ports.

The eight 802.3 Ethernet ports are 10BaseT (T for twisted pair) on the WS-C1201 model or 10BaseF (F for fiber) on the WS-C1211 model.

The switch can sit on a desktop, mount on a wall, or mount in an Electronic Industries Association (EIA)–compliant 19-inch open or closed rack.

Note Throughout this document, the Catalyst 1200 series switch is referred to as Catalyst Switch or the switch.

Summary of Features

Following are the features of the Catalyst 1200 series switch:

- Easy installation, configuration, and management
- Dual attachment station (DAS) with a single Media Access Control (MAC) address (single attachment station [SAS] configuration is also possible)
- Electronic Industries Association/Telecommunications Industry Association (EIA/TIA)-232 administration interface port (referred to as admin. port in this document)

Note Prior to the acceptance of the EIA/TIA standard by the ANSI committee, it was referred to as the RS-232 recommended standard.

- 10BaseT stackable unified management (SUM) port
- Ring and port status light-emitting diode (LED) indicators for all ports
- Nonvolatile memory for software configuration data
- 1 megabyte (MB) of Flash memory
- External optical bypass control switch capability
- Simple Network Management Protocol (SNMP) agent
- Downloadable software upgrades
- Remote access to the admin. port through support of Telnet
- Multiprotocol support (see the appendix "Supported Protocols and MIBs")
- Support for IP fragmentation during translation bridging
- Support for Management Information Bases (MIBs) (see the appendix "Supported Protocols and MIBs")
- Transparent bridging between Ethernet LAN segments or ports
- Translational bridging between Ethernet LAN segments and FDDI

- Institute of Electrical and Electronic Engineers (IEEE) 802.1d spanning-tree protocol
- Virtual LAN (VLAN) support for Internet Protocol (IP) routing with Routing Information Protocol (RIP)
- Access lists—intelligent frame filtering and custom filtering
- Port monitoring using the Switched Port Analyzer (SPAN)
- Remote monitoring
- IP multicasting support
- Support for SNMP MIB
- VLAN support for bridging
- IP Helper support for Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP)

The Catalyst 1200 series switch complies fully with FDDI Station Management (SMT) Specification Revision 7.3. A network administrator can monitor and control the switch from anywhere on the network using any SNMP management station.

Note Throughout this publication, CDDI refers specifically to the CDDI/MLT-3 standard.

Front Panel

The front panel of the switch has LED indicators for switch, ring, and port status as shown in Figure 1-1 and Figure 1-2.

Figure 1-1 Catalyst Series Switch—Front-Panel View (Plastic Panel Removed)

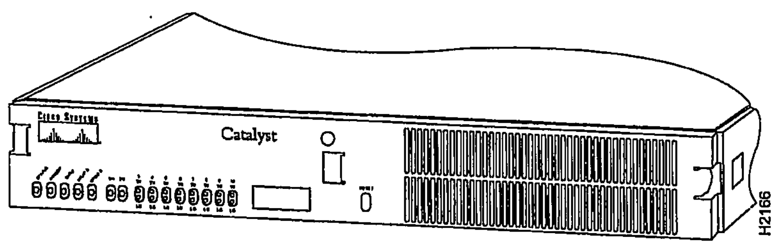
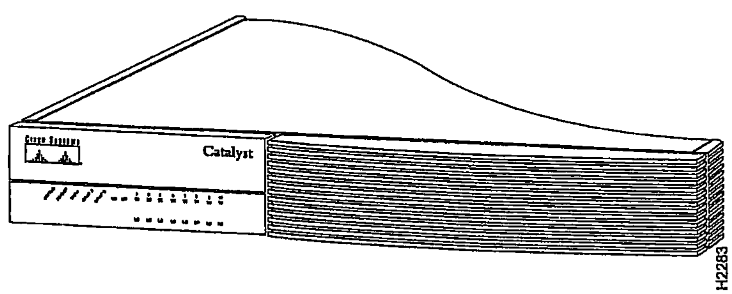


Figure 1-2 Catalyst Series Switch—Front-Panel View (Plastic Panel Installed)



Note The Catalyst 1200 series switch is shipped with the plastic front and side panels removed. Instructions for installing the front and side panels are included in the section "Wall-Mounting" in the chapter "Hardware Installation." The side panels are required for wall-mounting.

LEDs

Table 1-1 lists the descriptions of the front-panel LEDs, which are shown in Figure 1-3 and Figure 1-4. Use the LED descriptions in Table 1-1 to verify proper operation and for troubleshooting.

Figure 1-3 LED Indicators—Partial Front-Panel View (Plastic Panel Removed)

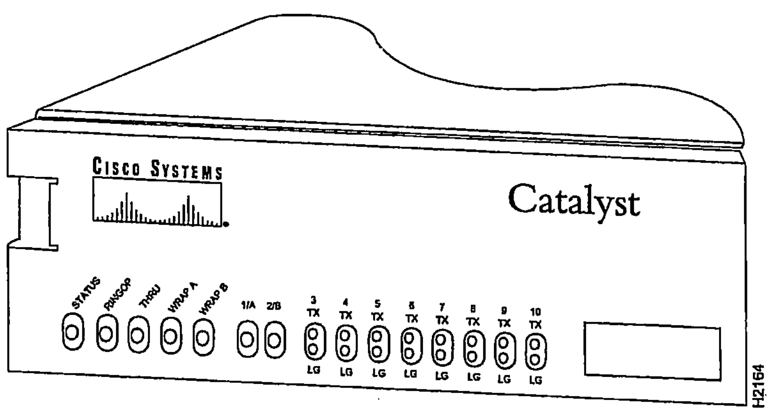


Figure 1-4 LED Indicators—Partial Front-Panel View (Plastic Panel Installed)

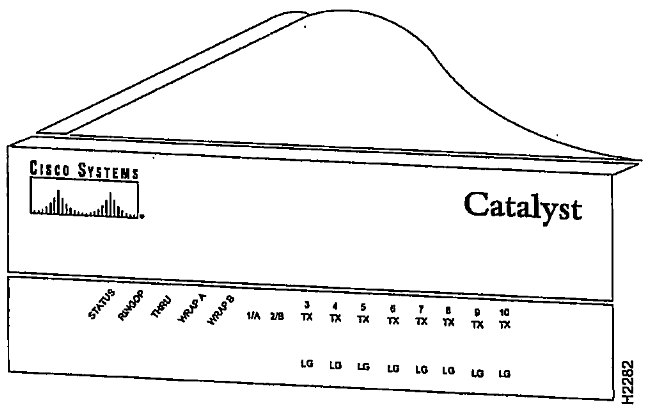


Table 1-1 Front-Panel LED Descriptions

LED	Description
Status	The switch performs a series of self-tests and diagnostics. If all the tests pass, the status LED is green. If any test fails, it is red (or orange for a minor fault).
Ringop	Indicates if the ring is operational. If the ring is operational, the ringop LED is green. If the ring is not operational, the ringop LED is off.
Thru	If the CDDI/FDDI A and B ports are connected to the primary and secondary rings, the thru LED is green; otherwise it is off.
Wrap A	If the CDDI/FDDI A port is connected to the ring and the B port is isolated, the wrap A LED is green; otherwise it is off.
Wrap B	If the CDDI/FDDI B port is connected to the ring and the A port is isolated, the wrap B LED is green; otherwise it is off.

LED	Description
Port 1/A status	If the CDDI/FDDI A port is connected to the ring, the port 1/A LED is green. If the CDDI/FDDI A port receives a signal but fails to connect, or a dual homing condition exists, the port 1/A LED is orange. The LED is turned-off if no receive signal is detected.
Port 2/B status	If the CDDI/FDDI B port is connected to the ring, the port 2/B LED is green. If the CDDI/FDDI B port receives a signal but fails to connect, or a dual homing condition exists, the port 2/B LED is orange. The LED is turned off if no receive signal is detected.
Port n TX[1]	Whenever an Ethernet port is transmitting a packet, the transmit (TX) LED is green for approximately 50 ms[2]; otherwise it is off.
Port n LG[1]	The link good (LG) LED displays the link integrity status of a LAN port. The LG LED is green if the link integrity is good. The LG LED blinks to indicate that a collision is detected on this link.

1. Where n is port number 3 through 10.
2. ms = milliseconds.

Reset Switch

Access to the reset switch, which is located behind the front panel, is through a small hole approximately one and a half inches to the right of the front-panel LEDs. (See Figure 1-5 or Figure 1-6.)

Figure 1-5 Reset Switch—Partial Front-Panel View (Plastic Panel Removed)

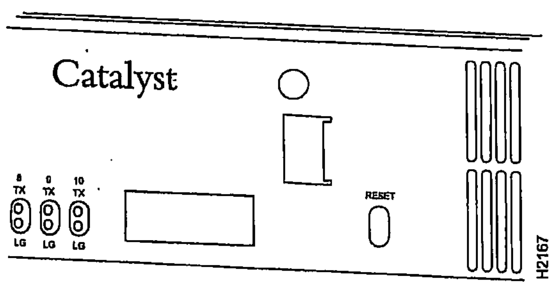
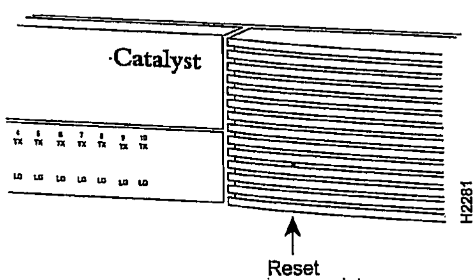


Figure 1-6 Reset Switch—Partial Front-Panel View (Plastic Panel Installed)

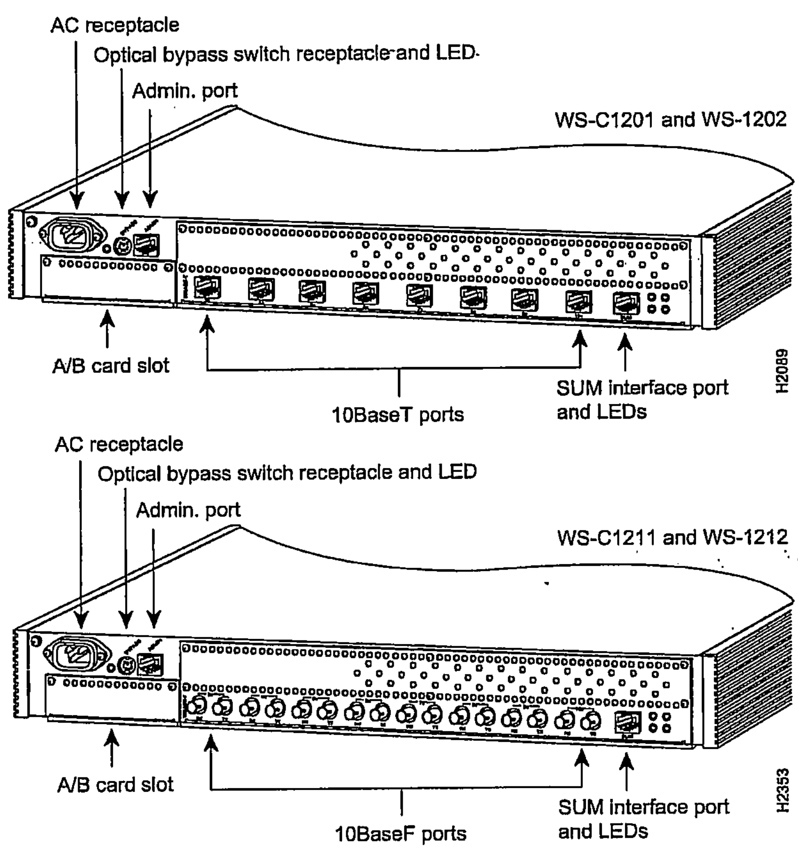


Note To reset the switch, use a thin tool (such as a small screwdriver) to press and release the button.

Rear Panel

The rear panel of the switch has an AC power receptacle, an optical bypass switch receptacle and LED, an EIA-TIA-232 admin. port, a card slot for an optional CDDI or FDDI A/B-port card, eight Ethernet 10BaseT (WS-C1201) or 10BaseF (WS-C1211) ports, and the SUM interface port (and LEDs). (See Figure 1-7.)

Figure 1-7 Catalyst Series Workgroup Switch—Two Rear-Panel Views



The chassis has no power ON/OFF switch. Power is applied when the power cable is connected between the switch and the AC source.

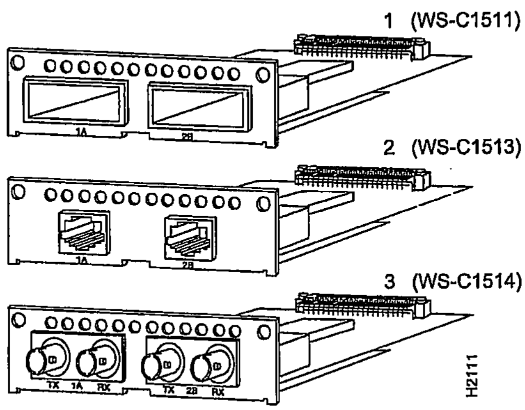
A/B Port Card Slot

The A/B card slot supports the following configuration: single-MAC DAS with dual homing configuration for FDDI (can also be used as an SAS). The A/B card slot also accepts CDDI/MLT-3 port cards. See Figure 1-8 for unshielded twisted-pair (UTP) and shielded twisted-pair (STP) connections.

Following are the three models of A/B port cards available:

- WS-C1511—DAS multimode FDDI, which accepts FDDI media interface connectors (MICs). (See 1 in Figure 1-8.)
- WS-C1513—DAS CDDI/MLT-3, which accepts category 5, UTP, modular RJ-45 connectors. (See 2 in Figure 1-8.)
- WS-C1514—DAS single-mode FDDI, which accepts standard FDDI ST-type connectors. (See 3 in Figure 1-8.)

Figure 1-8 CDDI and FDDI A/B Port Cards



The A/B port cards allow the switch to connect to a dual ring as a peer connection or to the master (M) port of another concentrator (cascaded tree configuration). To add an A and B port to the switch, insert an optional A/B port card. For A/B port card installation, see the chapter "Hardware Installation."

Power Receptacle

The power receptacle uses the AC power cord supplied with the switch. The power supply automatically accepts either 110 volts alternating current (VAC) or 230 VAC. To apply power, attach the power cord. To disconnect power, remove the power cord. There is no On/Off switch.

Optical Bypass Switch Receptacle and LED

The 6-pin mini–Deutsche Industrie Norm (DIN) connector is used to connect an external optical bypass switch to the switch. When idle, the optical bypass switch removes the nonfunctional dual attachment switch from the ring.

An activated bypass switch inserts the Catalyst Switch into the ring. Use an optical bypass switch only with the A/B port card option. If you install or remove an optical bypass switch, you must reset the Catalyst Switch. The bypass LED is on when the bypass switch is connected.

Admin. Port

The admin. port is the console terminal connection to the switch. To use the admin. port, connect an EIA/TIA-232 terminal (configured for 9,600 baud, no parity, eight data bits, and one stop bit), modem, or network management workstation. The admin. port enables you to perform the following functions:

- Configure the switch
- Monitor network statistics and errors
- Configure SMT and SNMP agent parameters
- Download software updates to the switch

Ethernet Ports

Ports 3 through 10 are IEEE 802.3 Ethernet 10BaseT (for the WS-C1201) or IEEE 802.3 Ethernet 10BaseF (for the WS-C1211). The 10BaseT ports use straight-through, RJ-45, modular UTP cables for connection to end systems, and cross-connect, RJ-45, modular cables for connection to other switches and concentrators. The 10BaseF ports use ST-type connections and multimode optical-fiber cable.

SUM Port

The stackable unified management (SUM) port is an out-of-band Ethernet 10BaseT port using a female RJ-45 UTP connection. The SUM port uses an RJ-45, modular, cross-connect cable when connecting to end systems; and straight-through cable when connecting to hubs. You can connect the SUM port to an Ethernet 10BaseT hub for Telnet, File Transfer Protocol (FTP), and SNMP management connection to the switch. For LED locations, refer to Figure 1-9. Table 1-2 lists the functions of the four SUM port LEDs.

Note The Catalyst Switch cannot bridge or route packets from a port to the console terminal connected through the SUM port.

Figure 1-9 SUM Port LEDs—Partial Rear-Panel View

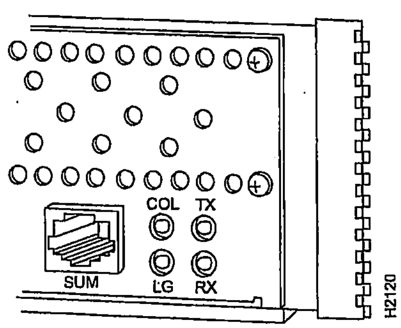


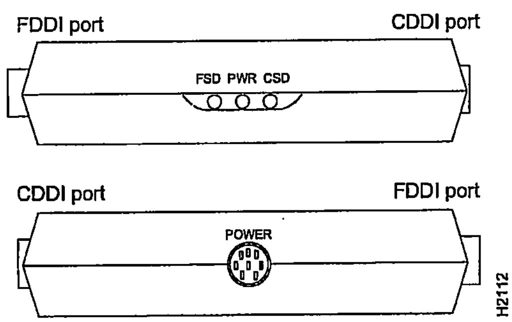
Table 1-2 SUM Port LED Descriptions

LED	Descriptions
COL	If collisions are detected on the SUM port connection, the yellow collision (COL) LED is on; otherwise it is off.
TX	If the SUM port is transmitting packets, the green transmit active (TX) LED is on; otherwise it is off.
LG	If Ethernet integrity is good, the green link good (LG) LED is on; otherwise it is off.
RX	If the SUM port is receiving packets, the green receive active (RX) LED is on; otherwise it is off.

CDDI-FDDI Translator

The optional CDDI-FDDI translator (model number WS-C703) provides a connection between CDDI and FDDI interfaces. The CDDI-FDDI translator includes an AC power adapter. The translator accepts an FDDI media interface connector (MIC) on one end and a CDDI (RJ-45) connection on the other end. Figure 1-10 shows two views of the translator.

Figure 1-10 CDDI-FDDI Translator—Two Views



One side of the translator has three status LEDs: FDDI signal detect (FSD), power (PWR), and CDDI signal detect (CSD). The other side of the translator has the power connector.

Technical Specifications

Table 1-3 lists the specifications for the switch.

Table 1-3 Technical Specifications

Specification	Description
Dimensions (H x W x D)	2.7 x 17.4 x 16" (6.96 x 44.2 x 40.6 cm)
Weight	17 lb (7.7 kg)
AC and DC	100 to 120 VAC, 2.0A maximum, 60 Hertz (Hz) 200 to 240 VAC, 1.0A maximum, 50 Hz 12A @ +5 VDC, 1A @ +12 VDC, 0.5A @ –12 VDC
Thermal dissipation	80W, maximum (273.04 Btus/hr)
Operating temperature	32 to 104 F (0 to 40 C)
Storage temperature	–40 to 167 F (–40 to 75 C)
Relative humidity	10 to 90% (noncondensing)
EMI[1] certifications	FCC Class A (47 CFR, Part 15) CISPR 22 Class A VDE Class A VCCI Class 1
Safety approvals	UL: 1950 CSA-C22.2 No. 950-M89 EN60950
Microprocessor	20 megahertz (MHz) 68EC030 for the NMP[2]
Memory	1 MB of Flash memory 4 MB of packet-buffer DRAM[3] 32 kilobytes (KB) of NVRAM[4]
Interface ports	Eight IEEE 802.3 Ethernet 10BaseF (WS-C1211) Eight IEEE 802.3 Ethernet 10BaseT (WS-C1201) A/B CDDI ports or A/B FDDI ports EIA/TIA-232 admin. port 10BaseT SUM port

Specification	Description
Network connectors	10BaseF (ST) 10BaseT (RJ-45) CDDI (RJ-45) FDDI (MIC or ST) Optical bypass switch: 6-pin mini-DIN SUM port: RJ-45 Admin. port: RJ-45
Network management	SMT 7.3 SNMP agent RMON agent (optional)
MIBs	See the appendix "Supported Protocols and MIBs"
LED indicators	Concentrator status Ringop Thru Wrap A Wrap B Traffic meter Link status (each link)
Maximum station-to-station cabling distance	625/125-micron multimode fiber: 1.24 miles (2 km) 50/125-micron multimode fiber: 1.24 miles (2 km) 8/125-micron single-mode fiber: 18.6 miles (30 km) Category 5 UTP[5]: 328' (100 m) IBM Type 1 or Type 2 STP[6]: 328' (100 m)
FDDI transmit power levels: Single-mode fiber	Average optical power: Maximum: –4.0 dBm[7] Minimum: –7.0 dBm
Multimode fiber	Maximum: –14.0 dBm Minimum: –18.5 dBm

Specification	Description
FDDI receive power levels:	
Single-mode fiber	Average optical sensitivity: –33 dBm Average maximum input power: –14 dBm
Multimode fiber	Average optical sensitivity: –34 dBm Average maximum input power: –14 dBm-

1. EMI = electromagnetic interference.
2. NMP = network management processor.
3. DRAM = dynamic random-access memory.
4. NVRAM = nonvolatile random-access memory.
5. UTP = unshielded twisted-pair.
6. STP = shielded twisted-pair.
7. dBm = decibels per milliwatt.

CHAPTER 3

Hardware Installation

This chapter provides complete hardware installation instructions for the Catalyst 1200 series switch. Before you install the switch, read the chapter "Preparing for Installation." The following topics are covered in this chapter:

- Overview
- Unpacking and inspecting
- Installing A/B port cards
- Removing A/B port cards
- Wall-mounting the switch
- Desktop placement of the switch
- Rack-mounting the switch
- What to do after the hardware is installed

Overview

Following is an overview of the hardware installation:

1. Unpack and inspect the switch.
2. Install the A/B port card (as required). Depending on your order, your system may been shipped with this card already installed.
3. If you are wall-mounting the switch or placing it on a desktop, install the front and side panels.

4 Install the wall-mount or rack-mount brackets on the switch.

5 Place the switch in a standard 19-inch rack, on a wall in a wiring closet, or on a desktop.

Warning Two people are required to lift the chassis. Grasp the chassis underneath the lower edge and lift with both hands. To prevent injury, keep your back straight and lift with your legs, not your back. To prevent damage to the chassis and components, never attempt to lift the chassis with the handles on the power supplies or on the interface processors, or by the plastic panels on the front of the chassis. These handles were not designed to support the weight of the chassis. To see translated versions of this warning, refer to the appendix "Translated Safety Warnings."

Note After the hardware is installed, refer to the chapter "Connecting to the Network" for information on connecting the ports to your network.

Unpacking and Inspecting

Before you install the switch, examine all shipping containers and contents for damage and check for missing items. If damage occurred to the containers during shipping, notify your carrier. Unpack and examine the contents of the containers. You should have the following items:

- The Catalyst 1200 switch
- This publication, *Catalyst 1200 Installation and Configuration Guide*

Note To order UniverCD, Cisco's library of product information on CD-ROM or printed publications, refer to *Ordering Cisco Documentation*, which is in your warranty package.

- AC power cord
- Modular cable with RJ-45-to-DB-25 adapter for the admin. port

- Rack-mount bracket kit
- Wall-mount kit (optional)
- Plastic front and side panels
- Warranty package

Fill out the warranty registration sheet and mail or fax it to Cisco Systems, Inc. today. Report any missing parts and any damage not related to shipping to your customer service representative.

Note Keep the packing materials for future use. *All components returned under warranty must be packed in their original packing materials.*

Installing an A/B Port Card

To install an A/B port card, perform the following steps:

Step 1 Disconnect power from the switch. If you handle port cards, properly ground the chassis to channel electrostatic discharge (ESD) voltages to ground.

Caution To prevent damage to a card, never install or remove a port card with power applied to the switch.

Step 2 Attach an ESD-preventive wrist strap.

Step 3 Remove the blank plate by removing the two Phillips screws.

Caution To prevent damage to the FDDI transceivers on the FDDI port card (in step 4), gently press down on the port card as you insert it so that the transceivers clear the chassis. The fit is snug.

Step 4 Slide the port card into the slot in the switch. Make sure the base plate slides *between* the guide rails in the switch. (See Figure 3-1.)

Carefully push the card into the slot until the card edge connector engages and the faceplate is against the rear panel of the chassis.

Warning Invisible laser radiation may be emitted from the aperture ports of the single-mode FDDI card when no cable is connected. *Avoid exposure and do not stare into open apertures.* To see translated versions of this warning, refer to the appendix "Translated Safety Warnings." Following is an example of the warning label that appears on the product:

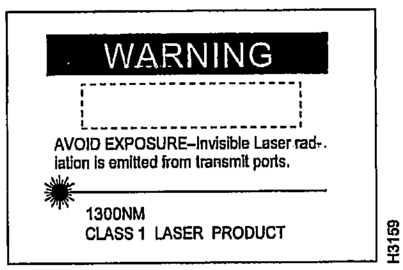
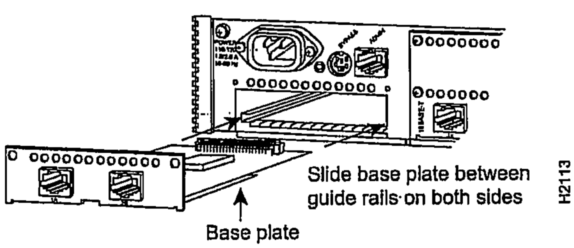


Figure 3-1 **Installing the A/B Port Card**



Step 5 Attach the card to the switch using two Phillips screws.

Step 6 Attach the appropriate interface cables to the port card.

Removing an A/B Port Card

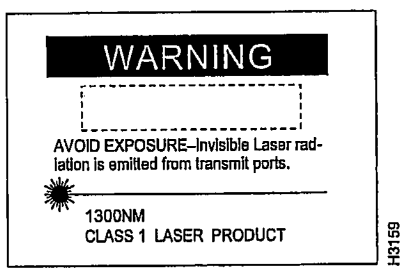
To remove an A/B port card, perform the following steps:

Step 1 Disconnect power from the switch. If you handle port cards, properly ground the chassis to channel ESD voltages to ground.

Caution To prevent damage to a card, never install or remove a port card with power applied to the switch.

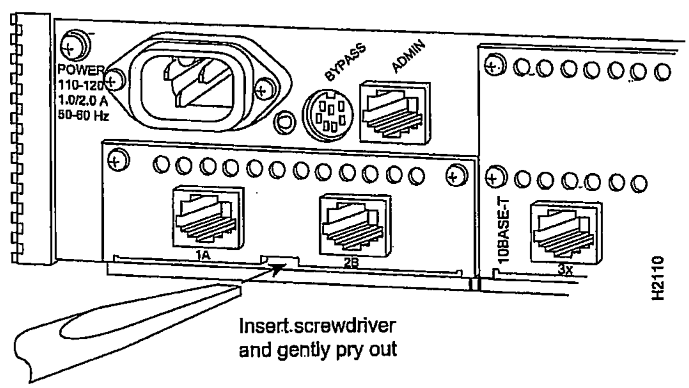
Step 2 Attach an ESD-preventive wrist strap.

Warning nvisible laser radiation may be emitted from the aperture ports of the single-mode FDDI card when no cable is connected. *Avoid exposure and do not stare into open apertures.* Following is an example of the warning label that appears on the product:



Step 3 Remove the two Phillips screws that secure the port card to the switch. (See Figure 3-2.)

Figure 3-2 A/B Port Card Screws



Caution To prevent damage to the FDDI transceivers on the FDDI-port card (in step 4), gently press down on the port card as you remove it so that the transceivers clear the chassis. The fit is snug.

Step 4 Gently pry the port card out of the slot with a flat-blade screwdriver. (See Figure 3-2.)

After traveling approximately 1/2 inch, the card is freed from the connector and slides out easily.

Step 5 Replace the blank plate.

Caution To help ensure proper airflow, operate the switch with either the blank plate or a port card installed.

Installing the Hardware

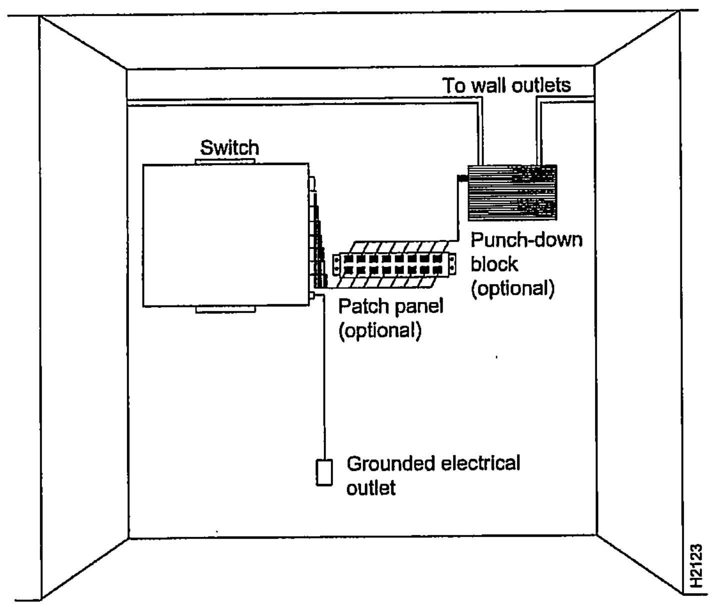
You can mount the switch on a wall, in a standard 19-inch rack, or place it on a desktop. Following are the procedures for wall-mounting the switch, installing it on a desktop, or mounting it in an open or closed rack.

Wall-Mounting

Figure 3-3 shows a typical wall-mount installation. The optional wall-mount kit consists of the following items:

- Two wall-mount brackets
- Four machine screws to secure the wall-mount brackets to the switch
- Four wood screws to attach the switch to the wall (you supply these)
- Wall-mounting template

Figure 3-3 Typical Wall-Mount Installation



To wall-mount the switch, perform the following steps:

Step 1 Remove the rubber feet from the switch if necessary.

Step 2 Mark the location of the four support screws that secure the switch to the wall. Use the template provided in the wall-mount kit. Make sure the screws attach to a wall stud or some other support that is strong enough to hold the weight of the switch.

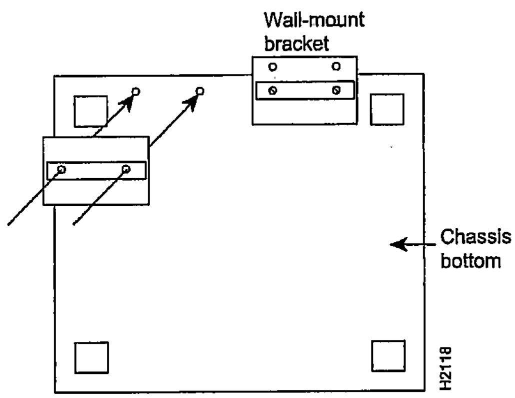
Step 3 Drill a pilot hole with a 1/16-inch bit at each mark you made for the location of a support screw.

Step 4 Screw the four 1/2-inch wood screws into the pilot holes, but not all the way; allow them to protrude about 0.125 inch (0.317 cm).

Step 5 Attach the wall-mount brackets to the switch with the machine screws supplied. Figure 3-4 shows where to install the brackets.

Caution Longer screws (longer than 0.375 inch [0.952 cm]) cause severe internal damage to the switch. Use the machine screws supplied with the wall-mount kit to attach the brackets to the switch.

Figure 3-4 **Attaching the Wall-Mount Brackets to the Bottom of the Switch**



Step 6 If the plastic front and side panels are installed, remove them from the switch. To remove a panel, hold it firmly with both hands and rock it slowly while you pull it away from the switch.

Step 7 Pick up the switch with the brackets facing away from you.

Step 8 Align the support screws with the holes in the brackets, and push the switch against the wall, allowing the screws to go through the holes in the brackets.

Step 9 Hang the switch from the support screws.

Step 10 Tighten the support screws to secure the switch to the wall. Do *not* overtighten them.

Step 11 Replace the front and side panels on the switch. To install a panel, hold it firmly with both hands and rock it slowly while you push it onto the switch.

Step 12 Continue with the section "What to Do After the Hardware Is Installed," later in this chapter.

Desktop Installation

The switch operates at a low noise level, which makes it suitable for any desktop environment. Place it in a clear and level location. Leave at least 3 inches (7.6 centimeters) clearance at the front for proper ventilation, and sufficient room at the rear for easy cable access. Proceed to the section "What to Do After the Hardware Is Installed" later in this chapter.

Caution To prevent damage from overheating, do not stack any other equipment on top of the switch chassis.

Rack-Mounting

The switch can also be mounted in an open or closed EIA-standard 19-inch rack using the rack-mount bracket kit. The rack-mount bracket kit consists of the following materials:

- Two L-shaped brackets
- Eight Phillips machine screws to attach the brackets to the switch

---

Note You provide the rack-mount screws.

To rack mount the switch, perform the following steps:

Step 1 If the front and side panels are installed, remove them from the switch. To remove a panel, hold it firmly with both hands and rock it slowly while you pull it away from the switch.

Caution Before you mount the switch in a rack, make sure of the following: the rack is secure and in no danger of falling over, the area around the rack does not exceed a maximum ambient temperature of 104 F (40 C), and sufficient airflow exists around the rack.

Warning To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. To see translated versions of this warning, refer to the appendix "Translated Safety Warnings." The following guidelines are provided to ensure your safety:

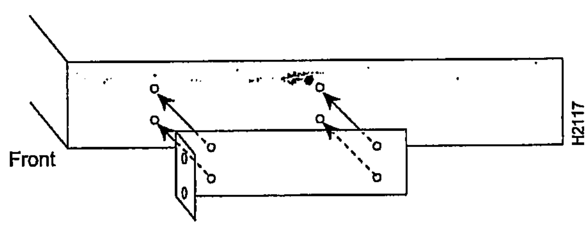
— This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

— When mounting this unit in a partially filled rack, load the rack from the bottom to the top, with the heaviest component at the bottom of the rack.

— If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Step 2 Attach a rack-mount bracket to each side of the switch with the supplied Phillips machine screws. Mount each bracket with the tab positioned toward the front of the switch. (See Figure 3-5.)

Figure 3-5 Attaching the Rack-Mount Brackets to the Switch



Step 3 Secure both brackets tightly, but do not overtighten them.

Step 4 Position the switch in the rack at the desired location and align the holes on the bracket tabs with the holes in the rack.

Step 5 Attach the switch to the rack using the screws you provide.

Step 6 Replace the front panel (if required) and store the side panels. To install the front panel, hold it firmly with both hands and rock it slowly while you push it onto the switch.

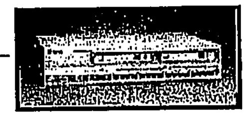
Step 7 Continue with the following section, "What to Do After the Hardware Is Installed."

What to Do After the Hardware Is Installed

After the chassis hardware is installed, continue with the chapter "Connecting to the Network" for the procedures required to attach all cables to the switch. Then go on to the chapter "Configuring the System" for the procedures necessary to configure the software portion of the system. For information on software commands, refer to the appendix "Command Reference."

Kalpana ProStack System

Click Picture for More Information.



- Stackable switching system for 4.8 Gbps of bandwidth
- Stackable bandwidth for Ethernet, 100 Mbps Ethernet, and 155 Mbps ATM
- Supports error-free cut-through technology
- Manage the ProStack system as a single entity
- Fault tolerant stackable switching
- Virtual LAN support within the stack
- Support for up to 10,000 MAC addresses
- Kalpana SwitchProbe network analyzer port
- Full-Duplex support on Ethernet, Fast Ethernet, and ATM
- Kalpana EtherChannel
- Address filtering
- Automatic address aging
- Teinet support
- SNMP MIB II, Ethernet MIB, and Kalpana extensions
- Flash PROM for software updates via bootp/TFTP or serial connection

---

PRODUCT OVERVIEW

Building on its expertise in Ethernet switching, Kalpana has developed the ProStack System, a high performance stackable switching platform. The Kalpana ProStack provides the user with a system that can be expanded as bandwidth demands dictate. The basic EtherSwitc@ol6 Ethernet switch supports 16 Ethernet ports, with expansion slots for two high speed modules. Using the ProStack Matrix, a cross-point switch, the user can expand bandwidth carrying capacity by connecting up to eight EtherSwitch Pro l6s for support of up to 192 switched Ethernet ports. By populating the expansion slots with high speed modules, the ProStack can support connectivity to Fast Ethernet and ATM.

The EtherSwitch Pro 1 6 breaks new ground in switch management. A new set of management options provide automated run-time and monitoring capabilities. Error-Free Cut-Through switching provides the low latency characteristic of cut- through switching with the data checking of store-and-forward switching. The EtherSwitch Pro I 6 can be configured on a per-port basis to automatically change from cut-through switching to store-and-forward switching if error rates exceed the user-defined threshold. This capability provides customers the best of both worlds, low latency cut-through switching and data protection.

The EtherSwitch Pro l6 is easily configured to meet users' unique network requirements. All interconnected EtherSwitch Pro 16s can be managed as a single SNMP entity, allowing users to configure address filters and Virtual EtherSwitch connections through a single console, Telnet, or SNMP session. Network statistics can be gathered on a per-port basis, either from the embedded Ethernet MIB or by using a SwitchProbe RMON agent connected to the EtherSwitch Pro l6. Either method provides the user with a wealth of information regarding the EtherSwitch Prol6 network operation.

HIGHLIGHTS

Error-Free Cut-Through Switching

Like all Kalpana EtherSwitches, the EtherSwitch Pro16 supports low latency on-the-fly or cut-through switching. It also supports automatic error-packet detection and elimination. Thus the EtherSwitch Pro 16 offers users the best of two worlds: the low latency characteristics of cut-through switching and the data checking capabilities of store-and-forward switching.

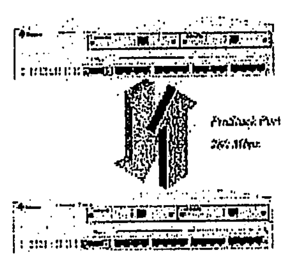
When switching between ports in the cut-through mode, the EtherSwitch Pro 16 reduces latency by forwarding packets as soon as their source and destination addresses are read. However, should CRC errors on a segment exceed the user-configured effor level, the offending port's operation automatically goes into the store-and- forward mode so that the bad CRC packets are discarded. When CRC errors on the segment fall below the threshold level, the port automatically reverts to the cut-through switching mode to optimize network latency.

Further error-free attributes allow the EtherSwitch Pro 16 to be configured to operate in runt-free operation. In runt-free mode, the EtherSwitch Pro 16 is configured to discard packets less than 64 bytes. This ensures filtering and elimination of collision fragments while maintaining the low latency characteristics of cut-through switching.

Stackable Bandwidth

Using the basic building block of the EtherSwitch Pro 16, the user is able to add switching ports and high speed connectivity. The EtherSwitch Pro16 supports sixteen 10 Base-T ports that can be individually configured for Full Duplex Ethemet. Bandwidth can be expanded by connecting two EtherSwitch Pro 16s together with the 280 Mbps Kalpana ProStack Port module at the Pro 16's back panel. Interconnecting two EtherSwitch Pro 16s with a cable provides connectivity for 32 10Base-T ports and four expansion slots.

For greater bandwidth demand, the user can connect up to eight EtherSwitch Pro 16s using the Kalpana ProStack Port and the ProStack Matrix cross-point switch. EtherSwitch Pro 16s can be added, automatically assuming the parameters of the stack, or removed, without disrupting stack operation. When EtherSwitch Pro16s are connected together, the entire stack is managed as a single entity.



Each EtherSwitch Pro16 expansion slot located on the front panel can be populated with a mix of modules to suit the user's requirement. If additional 10 Mbps ports are needed, the user populates the expansion slots with ProPort4T modules. If high-speed connectivity is required, the user selects the appropriate Fast Ethernet or ATM module. The following list illustrates the port-availability options:

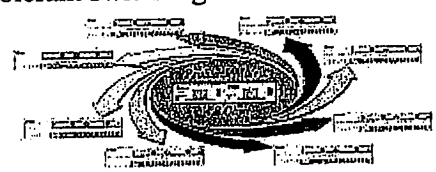
```
                Port Mix in a ProStack
--------------------------------------------------------------

                    | Ethernet Only |    Mixed Speeds    |
```

10 Mbps Switch Ethernet	192	128	128	128
Ethernet 100 Mbps		16		8
ATM 155 Mbps			16	8

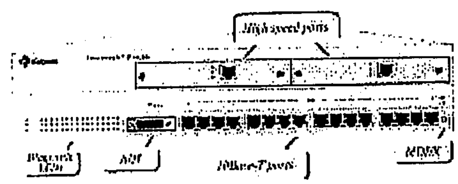
ProStack Matrix - Fault Tolerant Stackable Switching

The ProStack Matrix is an eight port, cross-point matrix switch designed to connect up to eight EtherSwitch Pro16 devices. The standard chassis supports one cross-port matrix module with a bay for the second, redundant module. Each module is a self-contained unit with its own logic and power supply. The redundant configuration provides the user with a fault tolerant switching fabric to ensure maximum uptime for the stack. Should the primary module go offline, the secondary module will detect and resume operation in less than one second, preventing lost sessions and reduced productivity.



EtherSwitch Pro16

The EtherSwitch Pro I 6 is a high performance stackable Ethernet switch. The chassis supports sixteen 10Base-T ports and slots for optional high speed modules. In addition, the Pro 16 can be expanded from a single switch to a high port-density stack of switches.



- **Kalpana EtherChannel**

  EtherChannel provides connectivity for existing Kalpana EtherSwitches by supporting multiple Full Duplex Ethernet links to the EtherSwitch Pro I 6. This capability allows users to retain their current equipment investment by providing existing EtherSwitches- the EPS-1500, EPS-2015RS, and EPS-2115M-high-speed connections to resources attached to the EtherSwitch Pro 16.

- **Virtual LANs Within The Stack**

  Both the EtherSwitch Pro 16 and Kalpana ProStack support Virtual EtherSwitch. The first step in providing Virtual LANs in an Ethernet network, Virtual EtherSwitch allows the user to designate specific ports to a Virtual LAN within the switch or the stack. Any communication between the designated Virtual EtherSwitches occur through a router, making each Virtual EtherSwitch a separate broadcast domain.

- **On-Demand Address Aging Per Port**

  Although each port on the EtherSwitch Pro] 6 supports up to 1,700 MAC layer addresses, there may be demand for a single port to support an even greater number of addresses. On-demand

aging, which allows users to set a threshold based on a specific time interval or a percentage of address table capacity, ensures that the port's address table is populated only by the most frequently used addresses. This capability allows users to transparently connect to high volume backbones.

- **Address Filtering**

  The EtherSwitch Pro16 supports the configuration of MAC layer filters on a per-port basis. This flexibility allows network managers to specify client access only to designated resources for security purposes. Filters can be for source or destination addresses. This allows the network manager to restrict access to certain servers or MAC addresses or to specify that an end user communicate with one and only one server.

- **Expansion Modules**

  Two expansion modules can be inserted into an EtherSwitch Pro 16. These modules can be used either for high-speed connectivity or for increasing the switched Ethernet port density.

  - New Fast Ethernet technology is provided by the ProPort 100T, which conforms to the IEEE 802.3U 100Base-TX standard and supports a single 100 Mbps port for Fast Ethernet over Category 5 cabling. Designed to provide connectivity to servers, routers, and workstations with 100Base-TX standard-compliant interface cards, ProPort 100T is user configurable to support Full Duplex Ethernet, for an effective throughput of 200 Mbps. The ProPort 100T has expanded buffers that support up to 2000 packets.
  - Low speed expansion modules are provided to support increased switched Ethernet port count. The ProPort 4T supports four 10Base-T ports. Each port is configurable to support Full Duplex Ethernet.
  - The ATM module, available in fourth quarter 1995, will initially provide connectivity between EtherSwitch Pro I 6s or ProStacks, creating a high speed ATM backbone. That support will be fol- lowed by LAN Emulation, which provides ProStack connectivity to an ATM enterprise network.

NETWORK MANAGEMENT

The ProStack System can be configured as an individual switch from the universal console port, Telnet session, or SNMP station. The EtherSwitch Pro 16's new network management features fit into two categories: automated run-time management and network- monitoring attributes. Run-time management capabilities include error-free cut-through switching; monitoring capabilities include support for the Ethernet MIB (RFC-1643), SwitchProbe, and RMON monitoring.

Network Monitoring

Statistics Gathering

The EtherSwitch Pro 16 introduces new levels of network management monitoring to switching products. The EtherSwitch Pro16 supports the Ethernet MIB, which allows users to characterize each port's broadcast packets, collisions, octets, utilization, and more. This feature provides the user with the detailed information characterizing an attached segment.

The EtherSwitch gathers statistics associated with each particular MAC address attached to the port. This feature allows the user to characterize user-specific segment traffic.

Further, Kalpana MIB extensions allow the user to gather data that associate a source or destination address with a port. This attribute permits the user to characterize the port-to-por-t traffic patterns with- in the EtherSwitch Pro 16.

Kalpana SwitchProbe Network Analyzer Port

The SwitchProbe port allows the user to connect a protocol analyzer or the Kalpana SwitchProbe RMON probe to the EtherSwitch Pro 16. Any single 1O Mbps port on the EtherSwitch Pro 16 can then be selected and monitored as if the probe or protocol analyzer were directly connected to that port. All packets are duplicated to the SwitchProbe port, whether the selected port is configured for Full or Half Duplex Ethernet.

THE ETHERSWITCH PRO16 GROWS AS NETWORK DEMANDS INCREASE

The stackable nature of the EtherSwitch Pro16 allows it to expand as network demands dictate. With a single EtherSwitch Prot 6, users can migrate a single collision domain Ethernet with 10 Mbps of throughput to 80 Mbps of throughput. A ProStack provides the user with up to 4.8 Gbps of network capacity to boost performance in the workgroup or department.

The EtherSwitch Pro16 has been designed to accommodate connectivity to existing Kalpana EtherSwitches using Full Duplex EtherChannel connections. Then, as network demands increase, high speed connections, either 100 Mbps Ethernet or ATM, can be installed for server and workstation connectivity.

As the number of workgroup connections increase, multiple EtherSwitch Pro 16s can be stacked to provide up to 192 switched Ethernet ports, with a mix of IO Mbps Ethernet to desktops and 100 Mbps Fast Ethernet to servers or workstations. Finally, ATM ports can be installed to interconnect Kalpana ProStacks or for connectivity to standard-based ATM switches.

Switch of Hubs

A typical starting application for the EtherSwitch Pro 16 is to resolve bandwidth congestion in the workgroup as a switch of hubs. Here, EtherSwitch ports are connected to existing workgroup hubs while servers receive their own 10 Mbps dedicated Ethernet. Connectivity to existing Kalpana EtherSwitches is provided by Full Duplex EtherChannel connections.

Switch of Servers

As end-user demands on the server increase, the network manager can improve server performance by giving each server a dedicated 100 Mbps connection. Inserting a 100 Mbps Fast Ethernet expan- sion module into the EtherSwitch Pro 16 increases server availability yet allows users to retain their current network technology and architecture. Each EtherSwitch Pro 16 can support two 100 Mbps Fast Ethernet connections.

Switch of Desktops

As network bandwidth and port-count demands continue to increase, additional EtherSwitch Pro 16s can

be stacked together to provide expanded connectivity. With the flexibility to provide up to 192 switched Ethernet ports in a single Kalpana ProStack, network managers have the option of providing users with a mix of shared Ethernet, dedicated Ethernet, Fast Ethernet, or ATM connections to servers or workstations. The Kalpana ProStack provides network capacity of up to 4.8 Gbps.

Interconnecting Multiple Kalpana ProStacks

As the network further expands, ATM or Fast Ethernet connections can be installed to provide connectivity to network backbones of multiple Kalpana ProStacks. And, as standards evolve, the ATM connection can be used to provide connectivity to standard-based ATM switches.

Send me some Information!

Back to the Products Page.

Kalpana ProStack Delivers New Stackable Architecture For Ethernet Switching

LAS VEGAS--(BUSINESS WIRE)--March 28, 1995--Cisco Systems, the worldwide leader in LAN switching, today unveiled the Kalpana ProStack system, a fault-tolerant, stackable LAN switching system that supports 10-, 100- and 155-megabit-per-second (Mbps) connections. Through Cisco's unique implementation of cut-through switching, which automatically detects and removes errors on a per-port basis, customers receive error-free transmissions without any degradation of switch performance.

The new ProStack system delivers up to 4.8 gigabits-per-second (Gbps) of bandwidth and consists of the EtherSwitch Pro16, a rack and stack Ethernet switch; the ProStack 100Base-TX Fast Ethernet interface module; the ProStack Matrix, an eight-port, non-blocking cross-point switch for connecting multiple EtherSwitch Pro 16s; and the Kalpana ProStack Port, an expansion module that provides connectivity to the ProStack Matrix.

Error-Free Cut-Through Switching

The EtherSwitch Pro16 can be configured on a per-port basis to automatically change from on-the-fly or cut-through packet switching, to store-and-forward switching if error rates exceed a user-defined threshold. When the error rate falls below the user-selected level, EtherSwitch Pro16 operation reverts back to cut-through switching.

Additional capabilities include a "runt-free" mode in which the switch discards packets less than 64 bytes. This ensures the filtering of collision fragments while maintaining the low-latency characteristics of cut-through switching.

"The Pro16 provides our customers with the best of both worlds -- the low latency of cut-through switching technology and the error protection provided by conventional store-and-forward technologies," said Larry Blair, director of market development. "By integrating these two technologies, we've made it easier for customers to build switching into corporate networks."

Expandable Bandwidth - Stackable Solution

Bandwidth can be incrementally expanded by interconnecting EtherSwitch Pro16s. The EtherSwitch Pro16 supports full duplex across all 16 10Base-T ports and two expansion slots for high-speed 100Base-TX, 100VG-AnyLAN or ATM connections. This combination of low- and high-speed connections enables users to create a fault-tolerant stack of up to 192 10-Mbps Ethernet connections. For added flexibility, each high-speed slot also may be configured with four switched 10Base-T ports or three 10Base-FL ports.

For mission-critical networks, the ProStack Matrix is available with a redundancy option. This consists of an additional self-contained module with complete logic and power supply. Should one module fail, the secondary module automatically begins operation within less than one second.

For existing EtherSwitch users, Models EPS-1500, EPS-2015RS and EPS2115M can be connected to the EtherSwitch Pro16 using EtherChannel connections. Assigning three full-duplex ports to one EtherChannel provides a "fat pipe" connection of 60 Mbps, optimal for many environments.

Easily Managed

The Kalpana ProStack Port and ProStack Matrix enable the stacked units to be seen and managed as a single device, even as new switches are added. Because the management is distributed throughout the stack, customers can easily add switches and view the entire system from a single console port, Telnet session or SNMP application.

Through Virtual EtherSwitch software, managers can assign specific ports anywhere within the stack into a virtual LAN domain. This simplifies desktop management by enabling nodes, like telephones, to follow users as they relocate within a facility. It also increases security by preventing ports in one Virtual EtherSwitch, or domain, from communicating with ports in another domain.

The SwitchProbe monitoring port allows a user to connect a protocol analyzer or the Kalpana SwitchProbe remote monitoring (RMON) probe to the EtherSwitch Pro16 to analyze traffic flow on any switched port in the stack. Thus, activity on switched half- and full-duplex LAN segments can be viewed from a centralized workstation.

In addition, full SNMP support ensures that the ProStack can be managed by a wide variety of third-party network management applications, as well as the Kalpana SwitchVision for Windows network management application.

Pricing and Availability

The EtherSwitch Pro16 is available in a standard or enhanced version. The standard EtherSwitch Pro16 includes support for SNMP, Spanning Tree Protocol and Address Filtering. The enhanced version adds full-duplex Ethernet, EtherChannel and Virtual EtherSwitch. U.S. list pricing and availability is as follows: -0-

CHAPTER 1

Product Overview

The Cisco 7000 router is part of the Cisco 7000 series. The seven-slot Cisco 7000 supports multiprotocol, multimedia routing and bridging with a wide variety of protocols and combinations of Asynchronous Transfer Mode (ATM), Ethernet, Fast Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), serial, High-Speed Serial Interface (HSSI), channel attachment, and multichannel media.

The Cisco 7000 has seven slots: five interface processor slots (0 through 4), one slot for the Switch Processor (SP) or Silicon Switch Processor (SSP), and one slot for the Route Processor (RP). There are bays for up to two AC-input or DC-input power supplies. Network interfaces reside on interface processors that provide a direct connection between the two Cisco Extended Buses (CyBuses) and your external networks.

Caution Due to agency compliance and safety issues, mixing AC-input and DC-input power supplies in the same Cisco 7000 is not recommended.

Note Your Cisco 7000 can also be optionally configured with a 7000 Series Route Switch Processor (RSP7000), which combines the routing and switching functions of the separate RP and SP. This new processor module requires that your Cisco 7000 also be configured with the 7000 Series Chassis Interface (RSP7000CI), which provides the environmental monitoring functions for the Cisco 7000. With this Cisco 7000 configuration, slot 5 (the 7000 RSP slot) is reserved for the RSP7000, and slot 6 (the 7000 CI slot) is reserved for the RSP7000CI. The remaining five slots (0 through 4) are reserved for interface processors. If your chassis was ordered with the RSP7000 option, both RSP7000-related components are installed when the Cisco 7000 ships. The RSP7000 functionality requires Cisco Internetwork Operating System (Cisco IOS) Release 10.3(9) or later.

Following is a list of acronyms that identify the system components and features:

- CxBus—Cisco Extended Bus. A 533-megabits-per-second (Mbps) data bus for interface processors.
- AIP—Asynchronous Transfer Mode (ATM) Interface Processor.
- CIP—Channel Interface Processor.
- EIP—Ethernet Interface Processor.
- FEIP—Fast Ethernet Interface Processor.
- FIP—FDDI (Fiber Distributed Data Interface) Interface Processor.
- FRU—Field-replaceable unit (as opposed to a spare part). A FRU can only be replaced by a Cisco certified technician. The arbiter board is categorized as an FRU; interface processors are categorized as spare parts.
- FSIP—Fast Serial Interface Processor.
- HIP—High-Speed Serial Interface (HSSI) Interface Processor.
- MIP—MultiChannel Interface Processor.
- OIR—Online insertion and removal. This feature allows you to replace interface processors and redundant power supplies without interrupting system power.
- PA—Port adapter. For example, the FSIP or MIP daughter card.
- RP—Route Processor. The system processor board.
- RSP7000—7000 Series Route Switch Processor.
- RSP7000CI—7000 Series Chassis Interface.
- SP—Switch Processor. The CxBus traffic controller.
- SSP—Silicon Switch Processor. The CxBus traffic controller.
- TRIP—Token Ring Interface Processor.

Figure 1-1 shows a view of the interface-processor end (rear) of the Cisco 7000 with AC-input power supplies, RP, and SP (or SSP) installed.

Figure 1-1 Cisco 7000 with RP and SP (or SSP), Rear View

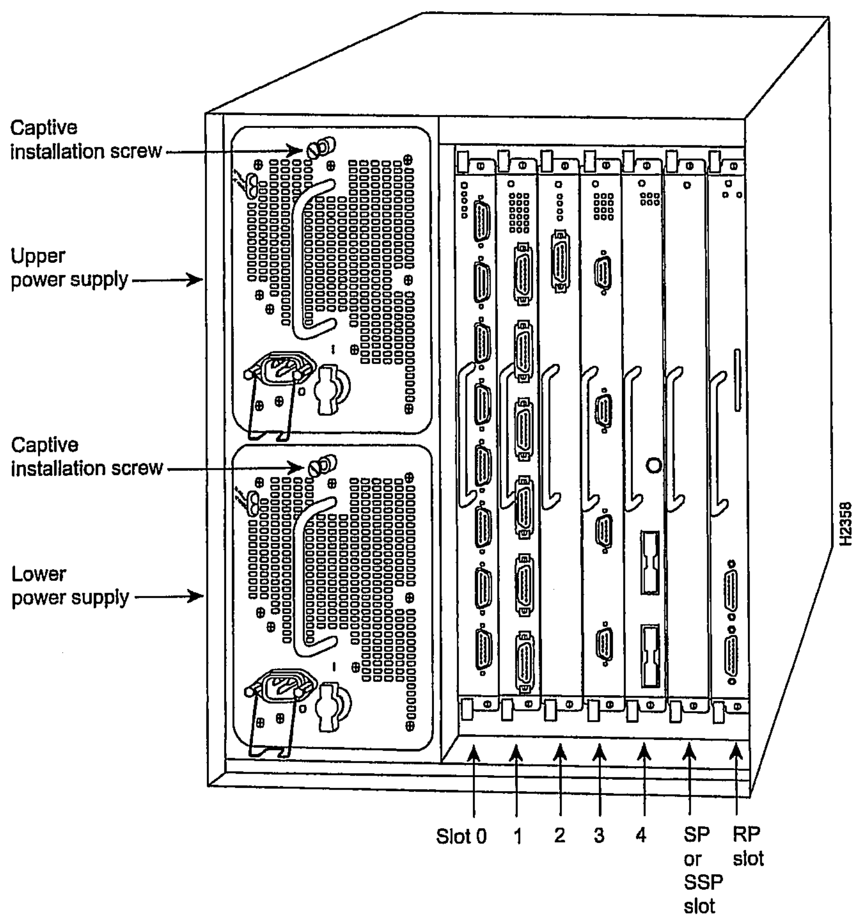
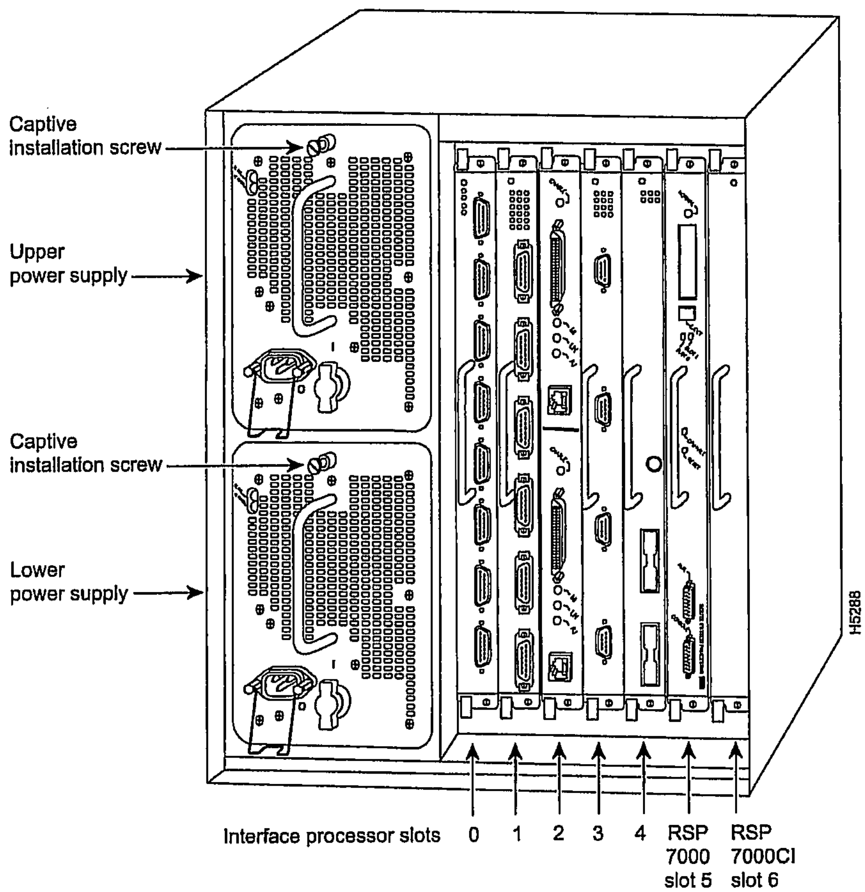


Figure 1-2 shows a view of the interface-processor end (rear) of the Cisco 7000 with AC-input power supplies, RSP7000, and RSP7000CI installed.

Figure 1-2 Cisco 7000 with RSP7000 and RSP7000CI, Rear View



System Specifications

Table 1-1 lists the specifications for the Cisco 7000 system.

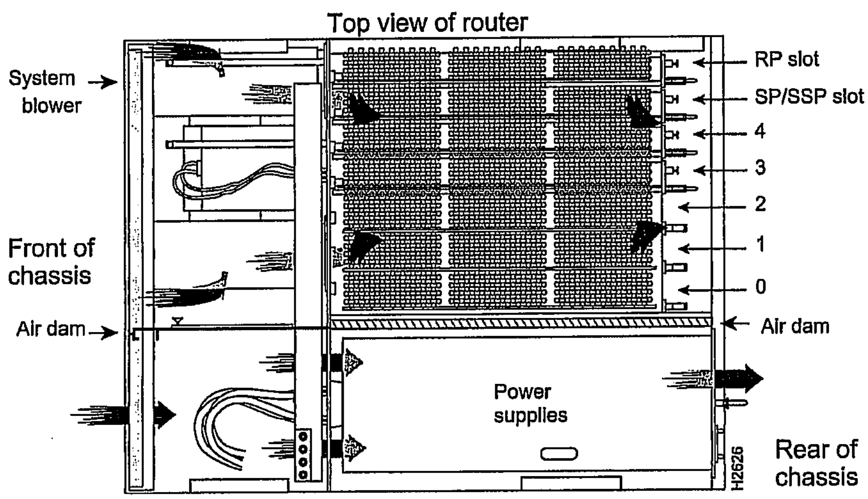
Table 1-1 Cisco 7000 Specifications

Description	Specifications
High-speed backplane	533-Mbps CxBus, 5 interface processor slots, 1 RP slot, and 1 SP (or SSP) slot
Dimensions (H x W x D)	19.25 x 17.5 x 25.1" (48.90 x 44.45 x 63.75 cm) Chassis depth including power cord is 28" (71.12 cm)
Weight	Chassis only: 76 lb (34.47 kg) Chassis fully configured with 1 RP and 1 SP (or 1 SSP), 5 interface processors, and 2 power supplies: 145 lb (65.76 kg)
Power supply	700 watts (W) maximum (for AC-input and DC-input power supplies)
Power dissipation	626W, maximum configuration 530W typical with maximum configuration
Heat dissipation	1200W (4100 British thermal units [Btus]/hr) with AC-input 300W (1024 Btus/hr) with DC-input
Input voltage	100 to 240 volts alternating current (VAC) wide input with power factor corrector (PFC)
Frequency	50 to 60 Hz autoranging
AC-input ratings	12A maximum @ 100 VAC, 6A maximum @ 240 VAC, chassis fully configured
DC-input ratings	–40 volts DC (VDC) minimum –48 VDC nominal –72 VDC maximum
Airflow	140 cubic feet per minute (cfm) through the system blower
Operating temperature	32 to 104 F (0 to 40 C)
Nonoperating temperature	–4 to 149 F (–20 to 65 C)
Humidity	10 to 90%, noncondensing
Agency approvals	Safety: UL 1950, CSA 22.2-950, EN60950, EN41003, AUSTEL TS001, AS/NZS 3260 EMI: FCC Class A, EN55022 Class B, VCCI Class 2

Airflow Considerations

The system blower on the Cisco 7000 provides cooling air for the processor modules. The blower is located inside the front chassis compartment, shown in Figure 1-3.

Figure 1-3 Cisco 7000 Blower and Airflow



The system blower draws air in through the air filter in the front chassis panel and directs it up through the floor of the internal slot compartment and over the cards. The exhaust air is forced out the rear of the chassis above and to each side of the processor slots. The blower needs a clean air filter in order to draw in sufficient amounts of cooling air; excessive dust in the filter will restrict the airflow.

Keep the air filter clean and replace it when necessary.

Sensors on the RP (or 7000 RSP) monitor the inlet and internal chassis air temperatures. If the air temperature at either of the sensors exceeds a desired threshold, an environmental monitor displays warning messages and can interrupt system operation to protect the system components from possible damage from excessive heat or electrical current.

The power supplies have their own fans. An air dam between the power supply bays and the processor module compartment keeps the airflow constant.

For complete information on fan and environmental considerations, refer to the *Cisco 7000 Hardware Installation and Maintenance* publication, which is available on UniverCD or can be ordered separately. For information on ordering UniverCD, see the section "If You Need More Configuration Information" in the chapter "Performing a Basic Configuration of the Cisco 7000."